Market Watch: Netbooks p. 79

Windows® IT Pro

JANUARY 2010 | WindowsITPro.com | W

UPGRADE YOUR DESKTOPS

The Path from Windows XP to Windows 7 p. 25

Cyber Threat Scanner: Detect Intrusive Files p. 56

Move Exchange to the Cloud p. 59

Supercharge PowerShell Search p. 63

Secure SharePoint Content p. 67

Restore AD Objects p. 35

Isolate Servers with IPsec p. 39

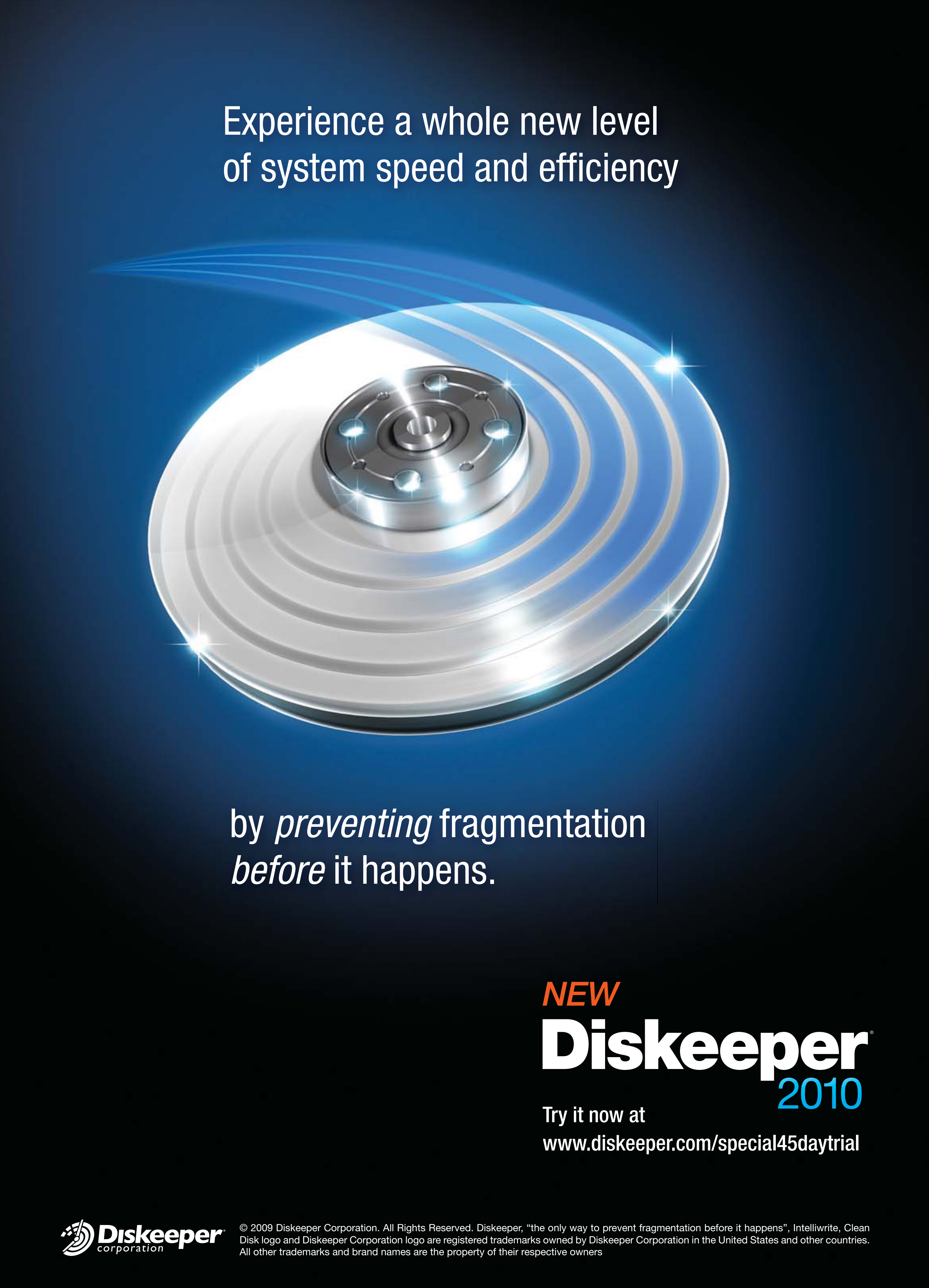
Solve PowerShell Argument Input Errors p. 45

Simplify EFS Deployment p. 49

Exchange Storage: DAS vs. SAN vs. iSCSI p. 53

Windows 7 Under the Hood: Interview with Microsoft Technical Fellow Mark Russinovich p. 31

PENTON
A PENTON PUBLICATION
JANUARY 2010
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

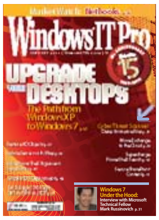


Experience a whole new level
of system speed and efficiency
by *preventing* fragmentation
before it happens.
NEW
Diskeeper®
2010
Try it now at
www.diskeeper.com/special45daytrial
Diskeeper corporation
© 2009 Diskeeper Corporation. All Rights Reserved. Diskeeper, "the only way to prevent fragmentation before it happens", Intelliwrite, Clean Disk logo and Diskeeper Corporation logo are registered trademarks owned by Diskeeper Corporation in the United States and other countries. All other trademarks and brand names are the property of their respective owners

C O N T E N T S

Windows IT Pro
A PENTON PUBLICATION
JANUARY_2010
VOLUME_16
NO_1

COVER STORY



FEATURES

INTERACT

IN EVERY ISSUE

COLUMNS

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

C O N T E N T S

PRODUCTS

Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director
Michele Crockett mcrockett@windowsitpro.com
Executive Editor, IT Group
Amy Eisenberg amy@windowsitpro.com
Technical Director
Michael Otey motey@windowsitpro.com
Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com
Web and Developer Strategic Editor
Anne Grubb agrubb@windowsitpro.com
Systems Management
Karen Bemowski kbemowski@windowsitpro.com
Caroline Marwitz cmarwitz@windowsitpro.com
Zac Wiggy zwiggy@windowsitpro.com
Messaging , Mobility, SharePoint, and Office
Brian Keith Winstead bwinstead@windowsitpro.com
Networking and Hardware
Jason Bovberg jbovberg@windowsitpro.com
Security
Lavon Peters lpeters@windowsitpro.com
SQL Server
Megan Bearly Keller mkeller@windowsitpro.com
Sheila Molnar smolnar@windowsitpro.com
Production Editor
Brian Reinholz breinholz@windowsitpro.com
IT Media Group Editors
Linda Harty, Chris Maxcer, Rita-Lyn Sanders

CONTRIBUTORS

News Editor
Paul Thurrott news@windowsitpro.com
SharePoint and Office Community Editor
Dan Holme danh@intelliem.com
Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com
Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond tony.redmond@hp.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Senior Art Director
Larry Purvis lpurvis@windowsitpro.com
Art Director
Layne Petersen layne@windowsitpro.com
Production Director
Linda Kirchgesler linda@windowsitpro.com
Senior Production Manager
Kate Brown kbrown@windowsitpro.com
Assistant Production Manager
Erik Lodermeier erik.lodermeier@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com
EMEA Managing Director
Irene Clapham irene.clapham@penton.com
Director of Sales
Birdie J. Ghiglione birdie.ghiglione@penton.com, 619-442-4064
Online Sales and Marketing Manager
Dina Baird Dina.Baird@penton.com
Key Account Directors
Jeff Carnes jeff.carnes@penton.com 678-455-6146
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883
Jacquelyn Baillie jacquelyn.baillie@penton.com 714-623-5007
Account Executives
Barbara Ritter barbara.ritter@penton.com 858-759-3377
Cass Schulz cassandra.schulz@penton.com 858-357-7649
Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953
Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service 800-793-5697 (US and Canada) 44-161-929-2800 (Europe)
IT Group Audience Development Director
Marie Evans marie.evans@penton.com
Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands Sharon.Rowlands@penton.com
Chief Financial Officer/Executive Vice President
Jean Clifton jean.clifton@penton.com

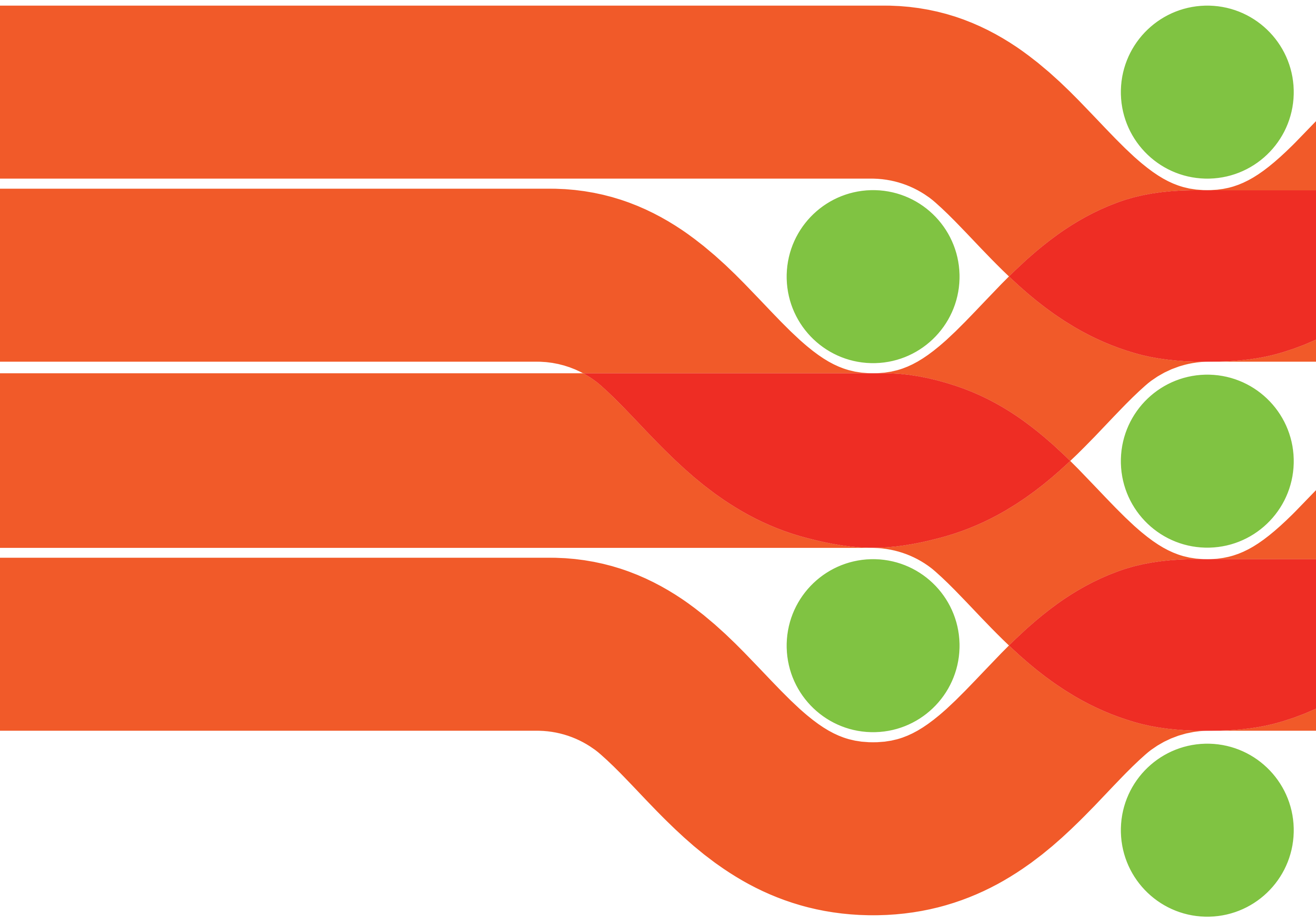
TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

REPRINTS
Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851



Crockett

"If hardware and software vendors can deliver solutions that save time and money, everyone wins."

In Pursuit of the Practical IT Pro

Focusing on economical IT solutions that work

After watching the reactions to last fall's Microsoft product releases and talking to software and hardware industry executives, I've concluded that the practical IT pro's approval is the most hotly pursued prize in the IT industry. It's no surprise given the past year's economic decline that questions about new products shifted sharply from "Is it cool?" to "Does it work?" The industry is scrambling to respond to IT pros' wish list for economical IT solutions that work.

IT pros have always been practical, but the industry is responding to IT pros' needs with unprecedented attentiveness. Microsoft's evangelism about its latest releases centered on the "New Efficiency" of deploying Windows Server 2008 R2, Windows 7, and Exchange Server 2010. The themes repeated by both Microsoft and third-party vendors included saving time and money, conserving energy, and increasing productivity—in other words, improving efficiency.

The changes aren't just catch phrases. At least in Microsoft's case, a shift in the process has put an emphasis on developing around complete scenarios—in which IT pros and end users can complete entire workflow processes—rather than viewing releases as collections of features.

Microsoft technical fellow and long-time *Windows IT Pro* author Mark Russinovich, who appealed to IT pros' practical side for years with his Winternals and Sysinternals utilities, recently observed that failing to focus on complete scenarios was one of Vista's downfalls. "A lot of scenarios people felt were left incomplete with Vista," Russinovich said. "It [was] nice and smooth up to this point, but then you're on your own." Russinovich contrasted this approach with the development of Windows 7, in which every component had to fit into "something useful for the customer." (For more of Russinovich's observations about the development of Windows 7, see "Windows 7 Under the Hood," page 31.)

Microsoft followed a similar discipline in developing Server 2008 R2, according to Bill Laing, Microsoft corporate vice president of the Windows Server and Solutions Division. "It's much more important to drive complete scenarios," Laing said. "You have to complete them." (Watch for a full interview with Laing in the February issue.)

Laing said that Microsoft used a customer-focused design methodology that started with interviewing customers and partners and recording everything they said—in their own words rather than Microsoft's. Laing said that a traditional pitfall of customer interviews is the tendency for the design team to interpret—and sometimes skew—the customers' message, yielding a result that too often is "what the person who interviewed them really wanted to build rather than what the customer wanted."

The second departure with the Server 2008 R2 and Windows 7 development approach was focusing on complete models that were "critical to quality" (CTQs, according to Laing). Rather than shipping when bugs were reduced to a specified number, the design teams focused on completing specific CTQs, such as being able to support a certain number of users in a VDI session. One workflow scenario that Laing said has drawn appreciation is the Active Directory Recycle Bin, which helps IT pros recover accidentally deleted AD objects.

Laing pointed out that many of the scenarios that emerged as most important were focused on cost savings. For example, Continental Airlines for years invested in executive lounges for its top customers. But now the typical CEO simply wants to get "from the car to plane, talking to as few people as possible," Laing said. Continental is using the new Microsoft technology to deliver customers' boarding passes directly to their cell phones. "People are now seeing that as a value as opposed to sitting in a lounge for two hours."

Both Russinovich and Laing referred to a development approach with these product releases that avoided disruptive changes—again, a tactic that caters more to the IT pro's peace of mind than to the cool factor. Laing said that Microsoft engaged with ISVs early in the process so that customers could more easily move applications into the Server 2008 R2 and Windows 7 environment without business interruptions.

Reducing power consumption was another extremely practical design objective with the new releases, resulting in core power management features such as Core Parking, which consolidates processing to the fewest number of processor cores possible and suspends inactive cores. It's a Prius rather than Porsche mentality. "The point is power management," Laing said. "It's more about miles per gallon than the top speed of the car."

As we start 2010, this practical design approach bodes well for helping IT organizations optimize operations to take advantage of the recovering economy. If hardware and software vendors can deliver solutions that save time and money, everyone wins.

InstantDoc ID 103181

MICHELE CROCKETT (michele.crockett@penton.com) helped launch *SQL Server Magazine* in 1999, has held various business and editorial roles within Penton Media, and is currently editorial and custom strategy director of *Windows IT Pro*, *SQL Server Magazine*, and *SystemiNetwork*.

- Hyper-V vs. VMware
- Upgrading Windows 7
- Virtues of R2
- Previewing PDFs

LETTERS@WINDOWSITPRO.COM

Virtualization Preference

I read Paul Thurrott's article, "What You Need to Know About Hyper-V 2.0," (November 2009, InstantDoc ID 102764), in which he maintains that Hyper-V 2.0 offers "an environment that's nearly as mature and full-featured as anything offered by VMware." Has Paul ever looked at VMware's offerings? Where are Hyper-V's distributed switches? How about fault-tolerant virtual machines (VMs)? Can Hyper-V support the installation of the Cisco Nexus 1000V to provide port-to-port management of virtual traffic? Does Hyper-V offer the advanced resource scheduling and pooling that vSphere does?

Both products are worthy of consideration, but to say that they're nearly the same is bewildering. Just because both products have a live VM migration option and can cluster doesn't make them nearly equivalent. That would be like saying a Kia is nearly the same as a Lexus because they both have engines and four tires. I've been a loyal *Windows IT Pro* subscriber since the late 1990s. This article and the shrinking size of the magazine will be contributing factors in my decision to renew the subscription.

—Brad Kulick

I've looked at VMware's offerings, and you're right: They're more full-featured and mature than Microsoft's. But that doesn't mean they're always the better choice. One obvious advantage of Microsoft's approach is that Hyper-V is provided for free as part of the base OS, thus democratizing the functionality and opening it up to a much wider audience than the high-end enterprises that would benefit from the features you mention. As long as you don't mind paying to play in its sandbox—paying a lot, in many cases—VMware does offer more. These days, of course, that's not always an easy sell. And for the growing upswell of small-to-midsized businesses (SMBs) that will soon mark the mainstream server virtualization market, that's arguably a more important consideration.

—Paul Thurrott

Regarding the size of the magazine, I have good news for readers. We're committed to delivering a robust print magazine and have made a commitment to add more editorial pages to Windows IT Pro *in 2010. The December 2009 issue reflected our increased folio, and you'll see a fatter magazine in your mailbox from this point forward.*

—Amy Eisenberg

Legal Windows 7 Upgrades

I read Paul Thurrott's commentary, "Microsoft: If You Use Windows 7 Upgrade Media to Do a Clean Install, You Could Be Breaking the Law" (InstantDoc ID 103057). I installed Windows 7 Professional clean on two computers by using the RTM Ultimate download from Windows Connect with the "delete ei.cfg" hack. I then re-armed twice until I received the two copies of Windows 7 Professional Upgrade I ordered during the half-price sale.

Now for the surprising part: Before messing around with installing over an existing installation, I tried something I didn't think would work—I went to Control Panel, System, Change Product Key and entered the keys from the upgrades. Lo and behold, both computers churned away for about a minute and successfully activated. Go figure.

—Bob Benedetti

Paul Thurrott states that "virtually every single PC user owns a previous version of Windows (Vista or XP) and thus qualifies for any upgrade version of Windows 7 and can install it any way they want, as long as they do so on the PC on which the previous version of Windows was installed and activated." I believe that statement is incorrect. The Windows 7 Upgrade EULA doesn't require that the upgrade be performed on the same PC that contained the previous version of Windows. In fact, paragraph 17 of the Upgrade EULA explicitly states that "you may transfer the software and install it on another computer for your use."

But what if the previous version was an OEM version? Doesn't the OEM EULA prohibit transfer to another PC? Paragraph 15 of the Windows 7 EULA explicitly states that "upon upgrade, this agreement takes the place of the agreement for the software you upgraded from." In other words, the Windows 7 EULA now overrides the OEM EULA. And, as we noted before, the Windows 7 EULA explicitly allows transfer to another PC.

To legally upgrade to Windows 7, you need only own an old PC with XP legally installed on it (it doesn't even have to work). You can then upgrade and transfer Windows 7 to any other PC. In fact, even if you had an old XP PC and threw out the hardware because it stopped working, you could use your old XP license to upgrade as long as you kept proof that you own a legal license. The Windows 7 EULA doesn't require that you own any hardware. All that's required is that "you must first be licensed for the software that is eligible for the upgrade."

I completely agree with Paul when he says, "I don't need Microsoft's approval, because the details are spelled out quite nicely in the Windows 7 EULA." It doesn't matter what Microsoft says. Windows 7 upgraders have rights under the EULA, including some rights they might not even know about. There's a lot of misinformation around. Please help publicize these rights.

—Alan Leow

InstantDoc ID 103208

continued on page 8

The Virtues of R2

I read John Savill's article "New Active Directory Features in Windows Server 2008 R2" (November 2009, InstantDoc ID 102483). It couldn't have come at a better time: I'm preparing to test R2. This excellent article helped me decide to migrate from Windows Server 2003 R2 SP2 to Server 2008 R2 instead of just Server 2008, which I have been contemplating for some time. Thank you!

—Jeff C. Watts

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

LETTERS@WINDOWSITPRO.COM

continued from page 6

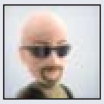
Preview PDFs in Outlook

I subscribe to the Tips & Tricks UPDATE newsletter, and just want to thank John Savill for a killer tip ("My PDF files don't preview correctly under 64-bit versions of Windows. How do I fix this?" Instant Doc ID 103038). I was frustrated that when running Windows 7 64-bit—or even Windows Vista 64-bit before that—I couldn't preview PDFs in Outlook 2007 as I could with 32-bit versions of the OS. John's tip saved the day. I can now preview PDFs in Outlook 2007 without opening them! Now, if John can just tell me how to make the PDF preview work for Windows Explorer, I'll be set!

—Jim Madaffer

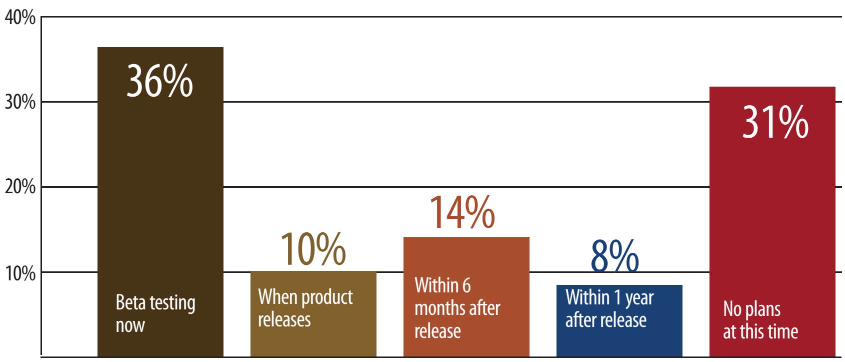
IT COMMUNITY FORUM

Read on twitter



devinganger Outlook 2010 rave: multiple Exchange accounts in one profile! Outlook 2010 rant: I have to exit Outlook to add them. PLZ FIX, KTHXBYE. Wednesday, September 23, 2009

Instant Poll Results:
When do you plan to migrate/upgrade your organization to Windows Server 2008 R2?



Source: *Windows IT Pro* Instant Poll, November 2009.

From the Windows IT Pro Magazine Forum on LinkedIn

Windows Server 2008 R2 Migration

When do you plan to migrate/upgrade your organization to Windows Server 2008 R2?

—Amy Eisenberg, Executive Editor

We will begin deployment of Windows 2008 by the start of 2009, and it will be a mix of Windows 2008 SP1/SP2 and 2008 R2. It will depend on our app vendors' support of the various versions of 2008, etc.

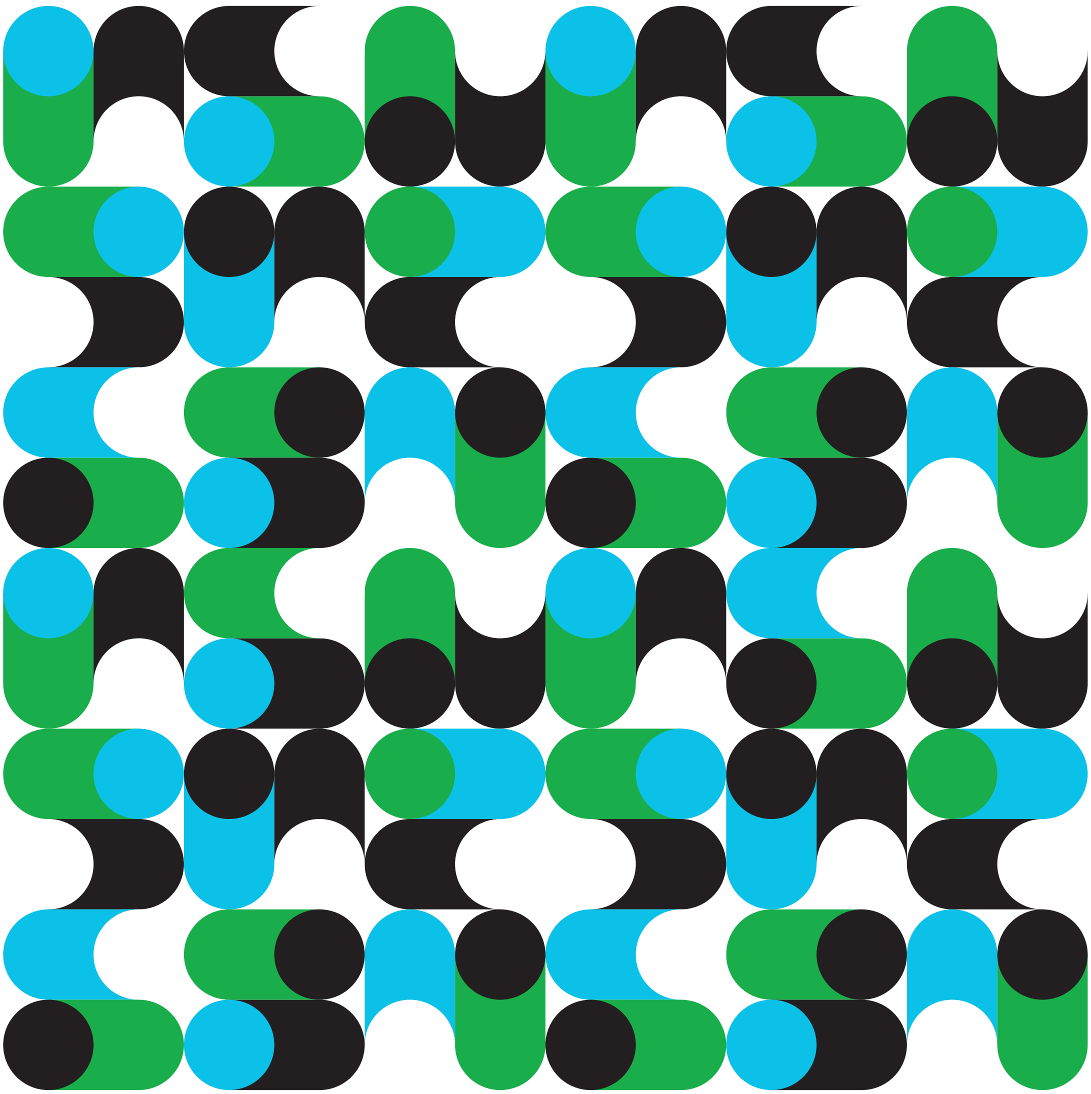
—Chris Wong

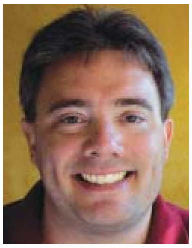
Already started deploying 2008 R2 as new server builds. We already have 6 servers (or 3 SQL clusters) in production. As we get new servers or rebuild servers already in production they are being built out as 2008 R2.

—Robin Hudson

We have already started the W2K8R2 deployments. We have 6 VM DC's in place and 5 application servers. We are looking to migrate to Exchange 2010 on the new platform in January 2010.

—Christa Wilson





Thurrott

"The 64-bit versions of Office 2010 take advantage of massive amounts of RAM, which should be of interest to Excel gurus."

What You Need to Know About Office 2010 Public Beta

With a public beta release of Office 2010 available, virtually anyone can get a look at a near-feature-complete version of Microsoft's next office productivity suite. Here's what you need to know about the Office 2010 public beta.

A Family of Products

Microsoft is really driving home the notion of integration across all of the products and services that make up the Office family of solutions. Yes, there is the traditional, PC-based productivity suite, of course, and standalone applications like Project and Visio, and these applications soldier on in Office 2010 with mostly evolutionary changes. But server products such as Exchange 2010, Exchange Online, SharePoint 2010, and SharePoint Online (and, of course, Office Communications Server) get major updates, with sweeping new areas of functionality. In the beta time frame, each of these products is available in near feature-complete versions (or, in the case of Exchange, final versions).

Office 2010 also includes the first generation of Microsoft Office Web Applications, such as Word Web App, Excel Web App, PowerPoint Web App, and OneNote Web App, and a new generation of Microsoft Office Mobile for Windows Mobile. They're not available in updated form for the beta, though Microsoft promises a pre release look in the coming months. (Microsoft is also working on the first version of Office Mobile for Nokia Symbian.)

Big Themes

In Office 2010, Microsoft is focusing on the fundamentals—copy and paste, email, and superior document fidelity and application integration—as well as what it calls tomorrow's expectations, those things that are forward-leaning today but could become core expectations for the future. These include the ability to work with high-definition imagery and video, real-time collaboration, and the ability to work anywhere, on any device.

Previous versions of Office integrated the new ribbon UI into several key Office applications. Now it will be available in all Office applications and even on the server; you'll see the ribbon UI in SharePoint 2010, for example. While some say they don't like the ribbon, Microsoft's metrics tell a different story of huge productivity gains for users. Over 12,000 third-party developers have signed on to add this UI to their own applications as a result.

But Office 2010 isn't just about the ribbon. Across various applications, you'll see such changes as a new BackStage environment that replaces the old File menu with a new full-screen interface for accessing all of the options related to the application and the current document. Many Office applications have gotten new image editing tools, and PowerPoint 2010 even provides surprisingly powerful video editing functionality.

New OpenType typography (Word, Publisher) provides for much more advanced control over type. And all Office 2010 apps pick up Paste Preview, which seeks to help those who use the number-two most-often-used Office command of all: Undo.

Also, in a first, Office 2010 will come with both 32-bit and 64-bit installers. The 64-bit versions of Office can take advantage of massive amounts of RAM, which should be of particular interest to Excel gurus. Excel can now handle spreadsheets with over 2GB of data.

Outlook's Update

In Office 2010, Outlook receives its biggest update in years. Although this is the one application in which the ribbon UI looks somewhat out of place, Outlook 2010 has enough new functionality to keep those of us who live in this application every day quite happy indeed.

A new Conversation View automatically organizes email messages by discussion. Excellent new tools like Ignore Conversation and Clean Up take the pain out of productivity-killing email threads, and Calendar Preview lets you view meeting participants' schedules in an inline mini-view so you can determine the best time for a scheduled meeting before you send the request off to everyone.

Another new Outlook 2010 feature, Quick Steps, provides a palette of customizable multi-step tasks. With just one click you can do such things as mark an email message as read, then archive it in a specific location. It's a huge time saver. And Outlook 2010 also supports the use of multiple Exchange accounts simultaneously.

Office 2010 on the Server

Some of the biggest gains in Office 2010 come from the server side. Exchange 2010 provides access to some of Outlook's best features—including MailTips, a feature aimed at preventing users from sending sensitive corporate data outside the company—as well as new features around Anywhere Access, unified messaging, email archiving, protection, compliance and more.

New to the public beta is a first peek at SharePoint 2010, which integrates more tightly into the individual Office 2010 applications. It also provides a new end-user solution, SharePoint Workspace 2010 (formerly Groove). Workspace can be used in tandem with SharePoint-based sites, and it can also be used to create ad hoc "server-less" SharePoint sites that let users collaborate over peer-to-

peer connections.

In the server itself, you'll see new developer extensibility capabilities, enhanced Internet site creation functionality (and new product versions aimed at those who wish to use SharePoint for public Internet sites), rich media support, and more.

Recommendations

While Office 2007 was a revolutionary release, Office 2010 feels evolutionary to me, with the exception of Outlook and SharePoint. But we won't have a full picture until updated prerelease versions of Outlook Web Applications and Mobile Office are made available.

For now, however, the public beta is an excellent chance to evaluate Microsoft's next-generation productivity solutions. If you're still using Office 2003 or earlier, you should look seriously at Office 2010. But even those on Office 2007 will find something to like.

InstantDoc ID 103119

What You Need to Know About Microsoft SQL Server 2008 R2

In keeping with its major/minor release cadence with Windows Server, Microsoft will soon deliver an interim update to Microsoft SQL Server 2008 called SQL Server 2008 R2. (A CTP release is now available for public testing.) SQL Server 2008 R2 builds on the solid foundation of its predecessor and provides access to the underlying improvements of the Windows Server 2008 R2 platform to achieve better-than-ever scalability, reliability, and performance. Here's what you need to know about SQL Server 2008 R2.

New Capabilities

A new self-service Business Intelligence (BI) capability lets Excel 2010 (and SharePoint 2010) users create their own BI solutions using the new PowerPivot feature (formerly code-named Gemini). This provides a way to aggregate a huge variety of data sources and data types, analyze them in memory, and work on millions of rows of data, even on a laptop. (This requires a 64-bit version of Excel; PowerPivot results can be published to SharePoint 2010 and shared with others.)

SQL Server 2008 R2 also provides for the central management of multiple SQL Server instances. The servers must be on the same network, but they don't need to be part of the same domain, and management is performed via Windows PowerShell or a new GUI tool.

Also, thanks to underlying platform improvements in Windows Server 2008 R2, SQL Server 2008 R2 offers stunning new scalability (both scale up and scale out) improvements. The server supports up to 256 processor cores now, and Microsoft has already published new industry benchmark records on 192 core systems. For data warehouses, SQL Server 2008 R2 supports massive parallel processing capabilities via "Project Madison," resulting in a new SQL Server product edition (see below). This functionality lets admins run queries over tens of billions of rows of data across multiple nodes in just seconds. Microsoft says that the scalability improvements in R2 make SQL Server relevant to 100 percent of any enterprise needs, up from about 99 percent in the original shipping version of SQL Server.

> With SQL Server 2008 R2, Microsoft finally blows past any remaining concerns about this product's ability to compete in the upper end of the market.

SQL Server 2008 R2 also provides "stream insight," a way to algorithmically query and process thousands of complex events simultaneously, providing actionable results in almost real time. This functionality can be used in places as diverse as web sites—where multiple users are navigating around and you wish to target task- or user-specific advertising—and oil refineries, where various levels need to be monitored and responded to in real time.

Finally, it adds Master Data Services (MDS), a portal and scorecard of sorts that provides a single view of customers, products, suppliers, or other data, all of which is aggregated across multiple systems. MDS (formerly code-named Bulldog) is the result of Microsoft's 2007 acquisition of Stratature, a provider of master data management software.

New Product Editions

SQL Server 2008 R2 will ship with a similar product lineup to its predecessor, with some changes. Microsoft is adding SQL Server 2008 R2 Datacenter and SQL Server 2008 R2 Parallel Data Warehouse editions to address high-end datacenter and data warehousing needs, respectively. And the previously available editions, SQL Server 2008 R2 Standard and Enterprise, gain a few new capabilities as well.

Recommendations

Like Windows Server 2008 R2, SQL Server 2008 R2 appears to be a very rich update with massive scalability improvements and useful functional enhancements, both of which belie the R2 moniker.

SQL Server 2008 R2 will interest the largest enterprises with mission-critical data needs or data warehouses. With SQL Server 2008 R2, Microsoft finally blows past any remaining concerns about this product's ability to compete in the upper end of the market.

InstantDoc ID 103094

PAUL THURROTT (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Minasi

"So far, I haven't unearthed the secret Server-Manager-to-DISM decoder ring."

Control Windows Features with DISM

The new feature-management tool Servermanagercmd.exe in Windows 7 and Windows Server 2008 has its pros and cons

After I set up my first Windows Server 2008 R2 system, I wanted to automate the addition of a few roles and features. So, I looked for the OS's Servermanagercmd tool to see how it worked under R2—only to find that it had been deprecated. In its place, Server 2008 R2 offers not one but two new command-line tools to add, remove, and modify roles and features: a set of PowerShell cmdlets (which require Microsoft .NET 3.5), and a standalone command called Deployment Image Servicing and Management (DISM), which doesn't need .NET. Managing features isn't DISM's only job, but I'll focus on feature control in this article.

DISM shows you all your system's possible roles and features and whether they're installed. To get that list, type

```
dism /online /get-features
```

DISM will spit out several screens of output; here's an excerpt:

```
Name : FaxServiceRole
State : Disabled
Feature Name : Printing-Server-Role
State : Enabled
```

In this example, you can see that I've enabled the role that DISM calls Printing-Server-Role—a role that Server 2008 R2 calls Print and Document Services in Server Manager—but left the Fax Server role disabled. (You'll sometimes have trouble figuring out which of DISM's names correspond to certain features; so far, I haven't unearthed the secret Server-Manager-to-DISM decoder ring.) To install the Fax Server role, I'd type

```
dism /online /enable-feature:FaxServiceRole
```

Servermanagercmd could install only one role or feature per command (unless you crafted some ugly XML to make it install multiple things simultaneously), but you can instruct DISM to install more than one role or feature with this slightly different syntax:

```
dism /online /enable-feature /featurename:<featurename> /
  featurename:<featurename>
```

For example, to install the fax service and the DNS server role in one command, you could type

```
dism /online /enable-feature /featurename:DNS-Server-Full-
  Role /featurename:FaxServiceRole
```

To remove a feature or features with DISM, just replace */enable-feature* with */disable-feature*.

DISM controls features on Windows 7, as well, so—for example—if you wanted to roll out Windows desktop images without any games, you could easily accomplish that with the command

```
dism /online /disable-feature:InboxGames
```

DISM also handles dependencies amongst roles and features. If you try to install a role or feature that needs another role or feature that isn't installed, it will ask you whether you want to install the necessary piece.

Servermanagercmd was a decent tool, but I never understood why Microsoft built it atop .NET, which guaranteed that Servermanagercmd couldn't run on Server Core and necessitated yet another command-line feature/role-configuration tool, OCSetup. DISM's designers were careful to make DISM as dependency-free as possible, which is why it not only runs on the full GUI-based Server 2008 R2, it also works well on Server Core R2 and even Windows Preinstallation Environment (PE) 3.0.

As you can see, DISM offers some good news, but it has some rough spots. The most annoying irritant is DISM's insistence on specific case in its feature names. For example, it wouldn't recognize

```
dism /online /disable-feature:inboxgames
```

Come on! Case-sensitive data processing went out with the Eisenhower administration.

I've already mentioned the lack of clarity between some of the feature names and their meanings, so be prepared to do a bit of homework when looking for the right words. What does BusScan-ScanServer refer to? Neither Google nor Bing offered any help, so all I can guess is that it's related to the new server feature that supports centralized scanners. Even if you focus on well-known roles such as DNS or DHCP, the names are puzzling or inconsistent: Why is DNS's name DNS-Server-Full-Role but DHCP's is DHCPServer?

Despite a few warts, DISM's ability to add or subtract sections of Windows will be extremely useful to anyone looking to automate rollouts. It's worth spending a little time to get to know it.

InstantDoc ID 103118

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books.

Otey

"I'll show you ten ready-to-use examples of Netsh commands for some of the most widely used network functions."

Network Configuration Tasks with Netsh

Simple commands to manage Windows Firewall, network adapters, and other system configurations

Netsh is a powerful and indispensible command-line tool for updating Windows network configuration settings. However, it can be confusing to work with. In this column, I'll show you ten ready-to-use examples of Netsh commands for some of the most widely used network functions. For more information about Netsh, download "Windows Server 2008 Network Shell (Netsh) Technical Reference" from the Microsoft Download Center at bit.ly/1iinSz.

10 **Show the system's current IP configuration**—You can use the following command to see if the system is using DHCP or static addressing as well as to show the system's current IP address, submask, gateway address, and DNS server:

```
netsh interface ip show config
```

9 **Configure a remote system**—Netsh can work with remote systems as easily as it can with local systems. The *set machine* command changes the computer that the Netsh command operates on to a different system on the network. For this command to work, you need to be logged on with an account that has administrative rights on the remote system:

```
netsh set machine win2ØØ8-2
```

8 **Working with IPv6**—Netsh commands work with both Windows IPv4 and IPv6 network stacks. To display your system's IPv6 address, use the following Netsh command:

```
netsh interface ipv6 show address
```

7 **Enable and disable Windows Firewall**—Netsh can work with the built-in Windows Firewall. In Windows Server 2008, the older Netsh firewall commands have been deprecated and replaced by the *advfirewall* commands. The following commands show how to disable then re-enable the Windows Firewall:

```
netsh advfirewall set currentprofile state off

netsh advfirewall set currentprofile state on
```

6 **Open a firewall port**—You can also use Netsh to open ports in the firewall for various applications. The following example shows how to open TCP port 1434 for Microsoft SQL Server:

```
netsh advfirewall firewall add rule name="SQL Server"
  dir=in action=allow protocol=TCP localport=1434
```

5 **Display network adapters and their status**—Many of the Netsh configuration commands require you to supply the name of the interface that you want to configure. The default value is usually Local Area Connection, but you can change this value. To find the name of the system's network adapters, use this commands:

```
netsh interface show interface
```

4 **Configure a network adapter to use a static IP address**—The following example shows how you use Netsh to set the IP address of the network adapter named Local Area Connection to 192.168.0.100, the subnet mask to 255.255.255.0, and the gateway address to 192.168.0.254:

```
netsh interface ip  set address "Local Area Connection"
  static 192.168.Ø.1ØØ 255.255.255.Ø 192.168.Ø.254 1
```

3 **Configure a network adapter with the address of a DNS server**—When you change the system's IP address type to static, you typically need to change the DNS configuration as well. This example shows how you use Netsh to configure the Local Area Connection to use a DNS server with the address 192.168.0.2:

```
netsh interface ip set dns "Local Area Connection"
  static 192.168.Ø.2
```

2 **Add a second DNS server to a network adapter's configuration**—Many networks use multiple DNS servers. To add a secondary DNS server with the address 192.168.0.3, use the following command:

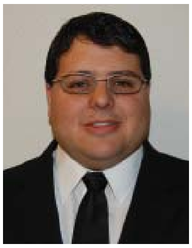
```
netsh interface ip add dnsserver "Local Area Connection"
  192.168.Ø.3
```

1 **Set a network adapter to use a DHCP-assigned IP address**—You can also use Netsh to set your system's network adapter to use a DHCP server for its IP address and to dynamically obtain the address of your network's DNS servers. This Netsh command configures your network adapter to use DHCP and DNS:

```
netsh interface ip
  set dns "Local Area Connection" dhcp
```

InstantDoc ID 103027

MICHAEL OTEY (motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).



Mangipano

"Bit flips that lead to bug checks are a common way that Windows detects a hardware problem (e.g., bad memory, an overheating CPU)."

Bit Flips: Was That a Zero or a One?

Learn how to recognize a common cause of bug checks that cause Windows system crashes

It's no fun when you're paged at 2:00 A.M. because your production server unexpectedly rebooted due to a bug check—a Windows system crash that can be caused by any of a number of conditions, such as malfunctioning hardware. But that's what happened to one server administrator when his hardware malfunctioned. The admin contacted Microsoft, and we analyzed the dump file. We found evidence of his hardware problem in the form of a bit flip. A bit flip occurs when you're copying data and one of the bits changes so that it's incorrect. A value of 1 incorrectly becomes a zero, or vice versa. Bit flips that lead to bug checks are a common way that Windows detects a hardware problem (e.g., bad memory, an overheating CPU).

In this article, I'll explain what a bit flip is and demonstrate an example of how we found one such bit flip, when a bit changed to an incorrect value as the CPU attempted to copy data, causing the system to crash. That way, if Microsoft support reviews your memory dump, and the support engineer explains that we found evidence of a hardware problem in the form of a bit flip, you'll have a solid understanding of what the engineer is talking about. I'll also provide some background information about access violations, registers, and the mov assembly language instruction.

Access Violation

The customer's server generated a memory.dmp file, which the customer submitted to the Microsoft Global Escalation Services team for analysis. I loaded the crash dump into the Windows debugger and began my review. (For more information about how to load a dump file into the debugger on your system, see "Administrators' Intro to Debugging," June 2009, InstantDoc ID 101818.)

Once the dump file was loaded into the debugger, I ran the command

```
!analyze -v
```

which provides basic information about the type of crash that occurred. The textual output from !analyze -v explained that invalid memory was referenced. Also, the debugger displayed the instruction that the CPU was attempting to execute when the crash occurred. This type of crash usually occurs when a pointer gets set to some value that it should not have been set to. Pointers should hold the address of where data is located in memory. If pointers are set to some bad value, the system can crash while attempting to follow that value. When this type of crash occurs as a result of the system accessing a garbage address, the crash is commonly referred to as an *access violation*.

The !analyze -v output has also listed the assembly language instruction that caused the access violation. In the output that Figure 1 shows, 80546944 was not a valid address, as indicated by the question marks shown next to the address. When the code that was running on the CPU tried to access this address, a page fault trap occurred, followed by an access violation.

Introducing the mov Command

Notice the mov command (which stands for move) in the output in Figure 1. Executing the mov command on the CPU copies the source to the destination. I'm not sure why this command wasn't called copy instead of mov, since the command doesn't delete the data from the source.

The mov command needs to know what data it must copy from and where to copy the data to. This information is provided in the form of operands. In the mov instruction in Figure 1, the EAX register is the first operand, and the first operand is the destination. (I'll explain what registers are shortly.) The second operand is dword ptr [esi]. This represents the address pointed to by the ESI register. How do we know that it is the address pointed to by ESI and not the ESI register itself? Because the debugger has surrounded the ESI register in brackets. The brackets tell us that the processor was not using the register itself but was instead using the contents of the register as a pointer to the virtual address where the data is located.

The debugger has also output dword ptr, which also tells us that the ESI register will be treated as a dword-sized pointer. Using a pointer as an address to get the actual data is called *dereferencing* the pointer. To summarize, the debugger has helped us identify that the command that was executing on the CPU when the crash occurred was trying to copy memory from the address contained in the ESI register to the EAX register. So there are registers with names, but what is a register anyway?

Viewing CPU Registers' Contents

Registers are small memory locations that are built into the

```
PAGE_FAULT_IN_NONPAGED_AREA (50)
Invalid system memory was referenced.  This cannot be protected by try-except,
it must be protected by a Probe.  Typically the address is just plain bad or it
is pointing at freed memory.
Arguments:
Arg1: 80546944, memory referenced.
mov     eax, dword ptr [esi]          80546944=????????
```

Figure 1: !analyze -v output showing access violation

CPU. They can be accessed very quickly as opposed to the amount of time it would take to access the memory located on the memory in slots on the motherboard slots (DIMMs, for example). Each of these registers has a name that the register is referred to, such as ESI or EAX.

You can use the *r* Windows debugger command to dump out the registers' contents. For example, if I run the r command from the debugger prompt and pass it the name of the ESI register, the following output will appear on screen, letting us know that ESI contains the value 0x86f4c658:

```
r esi
esi=86f4c658
```

If you scroll up to the !analzye -v output listed in Figure 1, you can see that this value contained in the ESI register is the value of the bad address. So the system crashed because ESI had a bad value loaded into it.

Examining the Previous Assembly Language Instruction

To understand why this particular system crashed, we will need to look at the assembly instruction that executed just before the bad value in ESI was accessed causing the crash. We can use the *ub* (unassembled backwards) command to look at the assembly language instructions that executed right before this instruction. Here's the command followed by its output:

```
0: kd> ub . L1
               mov esi, dword ptr [edi]
```

The period (.) tells the command to review the instructions backward starting from the current instruction. The L1 tells the command that we want to see only one instruction.

From the output, we can see that we followed a pointer in EDI to get the value that we're loading into ESI. Remember that the brackets around EDI indicate that we are dereferencing, otherwise known as *following*, a pointer contained in the EDI register. So now we know how ESI got the bad value. We copied the value from the memory location that EDI is pointing to. Let's use the *dd* (display memory as dwords) command to examine the data that EDI is referencing. Here's the command and its output:

```
1: kd>dd @edi L1
        80566944
```

The @ tells the command that EDI is the name of a register. The L1 modifier tells the command that we want to see only one dword.

So if the hardware had correctly performed the assembly language commands that the software instructed it to do, the value 80566944 would have been copied to the ESI register. Instead, as we showed earlier, the value present in the ESI register was the bad value, 80546944.

Breaking Down the Bits to Find the Bit Flip

Notice that the address is very close to the invalid address—80566944—that the instruction pointer was referencing. Let's use the debugger's built-in .formats command to convert these two values to binary format:

```
1: kd> .formats 80546944
  Binary:  10000000 01010100 01101001
  01000100
1: kd> .formats 80566944
  Binary:  10000000 01010110 01101001
  01000100
```

You can see that these two addresses differ by only one bit. As previously discussed, this type of error is known as a bit flip. It's caused by a hardware problem that causes one of the bits to be set to an incorrect digit.

Learning Path

More Windows troubleshooting articles in this series:

"Administrators' Intro to Debugging," InstantDoc ID 101818
"Conquer Desktop Heap Problems," InstantDoc ID 101701
"Disk2vhd: The Windows Troubleshooter's New Best Friend," InstantDoc ID 102980
"Examining Xperf," InstantDoc ID 102054
"Find the Binary File for Any WMI Class," InstantDoc ID 102615
"Further Adventures in Debugging," InstantDoc ID 102867
"Get a Handle on Windows Performance Analysis," InstantDoc ID 101162
"Got High-CPU Usage Problems? ProcDump 'Em!" InstantDoc ID 102479
"Reap the Power of MPS_Reports Data," InstantDoc ID 101468
"Resolve Memory Leaks Faster," InstantDoc ID 99933
"Resolve WMI Problems Quickly with WMIDiag," InstantDoc ID 100845
"Say 'Whoa!' to Runaway Processes," InstantDoc ID 100212
"Simplify Process Troubleshooting with DebugDiag," InstantDoc ID 100577
"Troubleshooting the Infamous Event ID 333 Errors," InstantDoc ID 101059
"Under the Covers with Xperf," InstantDoc ID 102263
"Disk2vhd: The Windows Troubleshooter's New Best Friend," InstantDoc ID 102980

A Bit of Understanding

As you've seen, understanding bit flips can help you better understand the underlying cause of a bug check that results in a system crash. By identifying when a bit flip has occurred, you'll have more detailed information to provide to Microsoft support, and you'll be able to hone in on the nature of a system crash (e.g., a hardware problem) more quickly. And, as a side educational benefit, you'll also gain some insight into the workings of Windows registers!

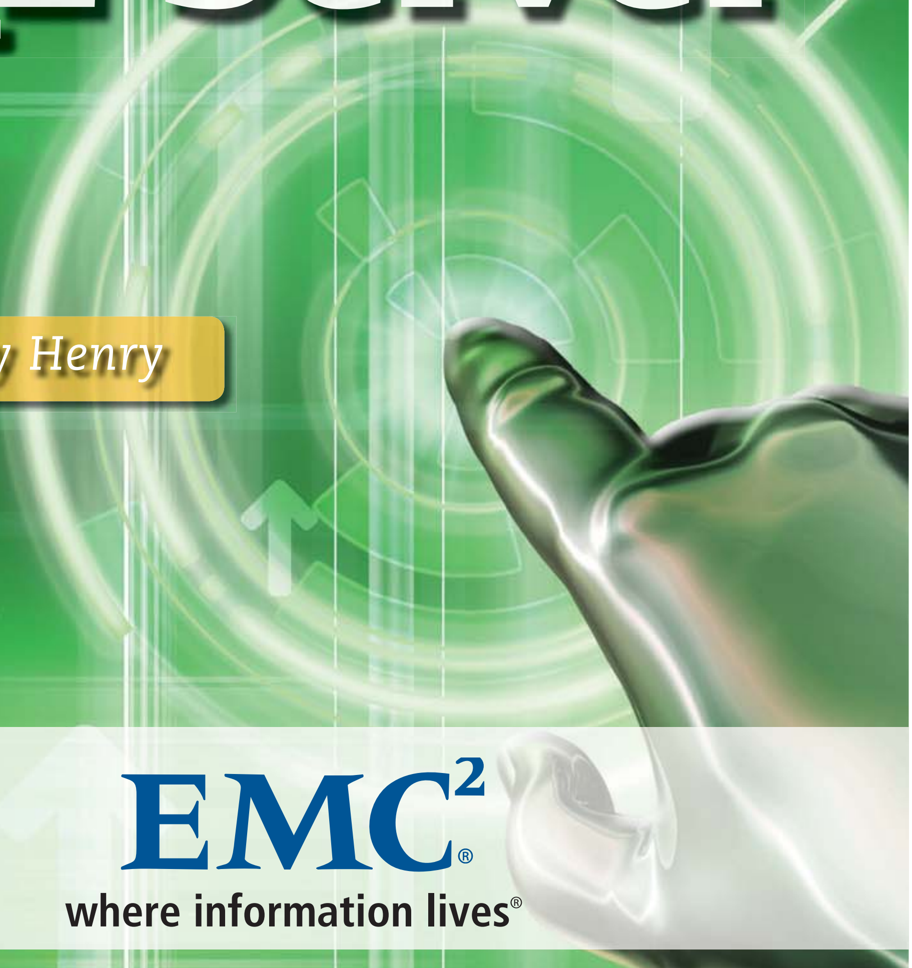
InstantDoc ID 103154

RYAN MANGIPANO is an escalation engineer on Microsoft's Global Escalation Services team in Las Colinas, Texas. He specializes in core Windows troubleshooting and advanced debugging. For information about Windows debugging, visit blogs.msdn.com/ntdebugging.

January 2010

The Essential Guide to Mission-Critical Microsoft SQL Server

By Wendy Henry



EMC²
where information lives®

SPECIAL ADVERTISING SUPPLEMENT TO *WINDOWS IT PRO* AND *SQL SERVER MAGAZINE*

The market demands today are forcing companies to operate smarter than ever before. Business information workers must make decisions quickly and decisively based on immediate access to accurate data. Additionally, recent regulatory trends and industry standards require many companies to securely archive their business data for lengthy periods while providing access to these archives for auditing. A popular platform for managing all of this business data, both archived and current, is the relational database management system, or RDBMS. And Microsoft® SQL Server® is one of the leading RDBMS Enterprise software applications on the market regardless of database size or performance requirements.

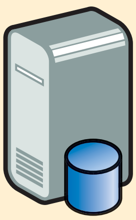
Today's Challenges in Data Management

A database in Microsoft SQL Server provides storage for several data types, including well-formed XML files (today's premier web file format). SQL Server databases also offer a myriad of management and scaling features, such as table partitioning, multiple data files per database, file/filegroup backups, clustered storage support, a full complement of backup and restore options and database replication. But choosing the right mix of features to enable in SQL Server, while keeping an eye on user demands and the company checkbook, can prove a daunting task. And choosing the appropriate storage architecture for SQL Server can impact critical SLAs for performance, scalability, and mission-critical data and service availability.

CROSS-REFERENCE
For more information about the features of Microsoft SQL Server, visit the product web site at: **www.microsoft.com/sqlserver**

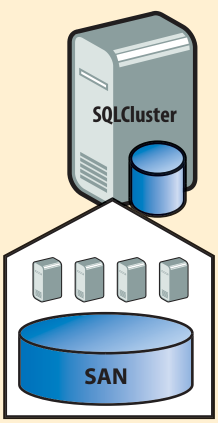
Architectural Considerations

The physical and logical architecture you choose for SQL Server can have a dramatic impact on the system's ability to grow with the business data. Be sure to choose an architecture for mission-critical databases that is flexible and scalable while providing the highest data availability and performance. Figure 1 describes a few architecture designs and their advantages and disadvantages. In fact, many companies turn to virtualization to reap high utilization ratios from their hardware



Single Server	Advantages	Disadvantages
Local Host OS	Simple	Limited Allocation
Local Hard Drives	Inexpensive	Limited Recovery Tools
Local SQL Install	Low Maintanence	Limited Scalability

Single Server	Advantages	Disadvantages
Guest OS w/SQL	Portable	Complex
Local Hard Drives	Independent from Host OS Storage Configuration	Requires Virtualization Software
Remote Storage	Fully Utilizes Resources	Requires Virtualization Management Tools



Cluster	Advantages	Disadvantages
Host OS w/Cluster App On Each Node	Automatic Failover	Complex
Remote Shared Storage	Workload Balancing	Costly
Cluster-aware SQL	Scalable	Prone to False Failovers
		Limited Geographically

Do You Know Why EMC is Your Partner of Choice for Microsoft SQL Server?

1. You are looking for a partner that understands both the Microsoft SQL Server platform and the information infrastructure that supports it.

EMC provides deep knowledge and best practices developed over almost a decade of experience with Microsoft SQL Server environments including both OLTP and BI/DW configurations. We also bring to the table thought leaders with elite Microsoft certifications, a broad range of expert services, a comprehensive information infrastructure portfolio—all supported by comprehensive alliance with Microsoft.

2. You seek a consultative approach to designing your next-generation deployments of Microsoft SQL Server and other key business applications.

EMC provides a complete portfolio of strategic consultation, planning, delivery, and support services across the entire lifecycle of your Microsoft SQL Server initiatives. Our consultants bring to bear a unique mix of industry, business, and technology expertise to solve your toughest challenges addressing business intelligence, data management, and OLTP requirements. We leverage customer experience, lab-validated EMC® Proven™ solutions, proven methodologies, best practices, and industry standards to minimize risk and increase efficiency across your SQL Microsoft lifecycle.

3. Your business demands a higher level of efficiency in its information infrastructure.

EMC solutions and technologies enable consolidation and simplified deployments along with cost-effective management and tiered storage efficiencies for the range of user data types and extreme data volumes that Microsoft SQL Server environments now support. With industry-leading technologies such as Virtual LUN and thin provisioning coupled with the broadest range of platform choices, EMC can help you address requirements for total cost of ownership, scalability, optimal utilization, and workload balancing. You need to ensure that the solution you deploy can meet your requirements for initial acquisition cost but also the cost of uptime, the cost of maintenance, and the cost of ongoing management. EMC delivers this via our leadership technologies for storage efficiency, including tiered storage with table partitioning and fully automated storage tiering.

4. You want to leverage virtualization to lower TCO and improve agility and flexibility.

EMC is a leading Microsoft consultancy with storage technology integration across Microsoft's product portfolio, and deep experience in information infrastructure for virtual environments supporting both VMware® and Microsoft Hyper-V™. EMC has the technologies, solutions, and expertise to help you fully leverage the benefits of virtualization for SQL Server consolidation—and improve utilization addressing load distribution using VMware DRS, HA, and Hyper-V technologies such as Live Migration. Deploying virtualized Microsoft applications with an EMC storage infrastructure can create the efficient, protected, and easy-to-manage environments you need to address current and future requirements.

5. You need to ensure data protection with robust backup, recovery, and restore solutions.

EMC has a complete offering for backup, recovery, and restore that includes tiered service levels for performance and recovery, disk-based recovery options, integration with point-in-time replication, and advanced software solutions for recovery management. These advanced tools offer LAN-free data protection solutions that are tightly integrated with Microsoft applications and Microsoft SQL Server software—including support for multi-site clustering using storage-based replication (cluster enabler) and disk-based replication for backup acceleration, reporting, and analysis services optimization.

6. You must ensure business continuity.

EMC has deep experience across diverse customer environments in high-availability and business-continuance solutions for Microsoft SQL Server environments, combining hardware platform reliability with advanced replication software capabilities. And EMC's local and long-distance replication solutions are validated and supported by reference architectures and proven best practices. EMC solutions and technologies extend high availability across multiple sites with near-zero downtime with cluster enabler integration. EMC solutions also ensure continuous data protection and multi-site, SQL-aware bookmarks for any point-in-time recovery with EMC RecoverPoint CDP.

7. You want to partner with an industry leader in Microsoft SQL Server deployments.

A Microsoft Gold Certified and Global Alliance Partner with 11 Microsoft competencies and 20 "Partner of the Year" awards, EMC works with Microsoft to develop best practices that combine software—hardware, and services to help you streamline deployment, migration, and management of your Microsoft platform. Together, we help deliver the higher levels of information protection and access your business needs while increasing efficiency and lowering risk.

8. To reduce risk, you want a partner with validated best practices and technology solutions to ensure deployment, upgrade, and migration initiatives are delivered in a predictable manner.

To ensure EMC products perform at the highest levels, we conduct the industry's most comprehensive interoperability testing. We're committed to developing and testing hardware and software products that are fully qualified with Microsoft technologies, supporting Microsoft users with compatible, integrated solutions.

9. You need to accelerate the business value of Microsoft SQL Server.

Whether you're deploying, upgrading, or migrating to Microsoft SQL Server you can accelerate the entire process and ensure exceptional results with EMC Solutions for SQL Server. With the enterprise-grade capabilities of Microsoft SQL Server and a powerful EMC storage infrastructure, you can reduce complexity and enable advanced consolidation throughout your entire organization.

10. You want to work with a partner that has global reach to support your Microsoft SQL Server environments.

EMC's Global Services organization has thousands of consultants with deep expertise to provide a broad portfolio of strategic consultation, planning, delivery, and support across the entire IT lifecycle from envisioning through day-to-day operations.

and storage investments while maintaining acceptable resource performance counter values. Virtual SQL Servers look, walk, and quack just like independent server equipment to the rest of the network but provide a layer of abstraction from the actual host OS running large-capacity servers. The ability to quickly port virtual machines from one piece of hardware to another makes virtual SQL Servers attractive for mission-critical data because they can easily be moved or replicated to larger or closer storage facilities. Virtual machines and the SQL Server instances installed on them can also be taken offline as archives.

Controlling Data Bloat

SQL Server online transaction processing (OLTP) databases are typically write-intensive. And like any system subject to user input, SQL OLTP databases are vulnerable to data bloat. Duplicate values, antiquated data and unnecessary information placed into a SQL Server database can cause it to grow to an unmanageable size, affecting performance as well as infrastructure costs. One of the best deterrents to data bloat is user training, but consolidating SQL instances or databases can also positively impact overall IT infrastructure and resource utilization. Additionally, providing users with intuitive navigation, relevant search platforms, and understandable data presentation solutions can mitigate data bloat.

The Business Intelligence (BI) Balancing Act

Providing information workers with business intelligence data from SQL Server is a critical business requirement—but it must be balanced with the existing production workload. While the demands of users seem infinite, realistic expectations should be set regarding access time, summarization, and detail levels of the information. For example, retrieving summarized data requires CPU cycles on the SQL Server to aggregate the summarized results but returning detailed data sets burdens the storage and network substructures of the equipment. Large data warehouses constructed using online analysis processing (OLAP) solutions—such as SQL Server Analysis Services that store summarized business information—require fast devices with large storage capacity to deliver analysis data to users efficiently. In fact, populating the data warehouse can be automated to occur during off-peak hours when contention for the infrastructure is less likely.

Doing More with Less—Leveraging Automation and Virtualization

Microsoft SQL Server is a true enterprise-class relational database management system. It includes intuitive GUI management tools and lowers the cost of owning a data management system by incorporating automation and delegation of administrative tasks. The application scales at the owner's pace, is cluster-aware, and takes advantage of large hard drives by invoking a small data page on the drive to reduce overhead and wasted space. Microsoft SQL Server is also a candidate for virtualization, allowing SQL administrators to arrange SQL instances without being limited by host operating systems or their storage layouts. When compared with its competitors in the same market space, Microsoft SQL Server provides more enterprise-class features for less purchase price and total cost of ownership than many other RDBMS platforms.

Infrastructure Considerations for SQL Server

Regardless of your chosen topology for SQL Server, there are specific storage and infrastructure considerations that can impact your SQL Server's performance and the availability of mission-critical business data. Your challenge is aligning the most appropriate solution (including the various hardware choices and software options) to your business requirements. Because the data in SQL Server is often critical to daily business continuity as well as invaluable as decision-making criteria, it is imperative that the SQL Server remain available to end users as much as possible. In fact, you should seek Microsoft-endorsed infrastructure and storage partners like EMC who provide complete end-to-end expertise across SQL Server and the infrastructure. EMC offers expertise and infrastructure solutions that support mission-critical applications, minimize downtime, and provide feature-rich management tools to enable operational efficiency. EMC also works with Microsoft to invest in developing joint best practices and integrated solutions to help their customers derive even greater ROI and lower TCO for Microsoft SQL Server environments.

CROSS-REFERENCE

For more information on EMC solutions for SQL, go to **www.emc.com/sql**

Infrastructure Considerations

One of the most common storage solutions for SQL Server is a SAN. However, traditional SAN storage used a single drive host in direct communication to the SQL Server's host OS. This unilateral, single-hierarchy design left the solution vulnerable to single point of failure (the communication path or the host device) and questionable disk partitioning practices such as short stroking to reduce seek times. Newer tiered SAN designs allow companies to make the most of multiple SAN purchases by layering them to the network, fully utilizing storage and introducing duplicity to the communication and host chain, eliminating single point of failure.

When choosing a SAN solution for SQL Server, be sure to look for:

- dynamic allocation capabilities such as thin provisioning that allow logical areas to be defined for SQL Server without being reserved on the actual SAN, enabling the footprints on the drives to remain until needed and reassigned to alternative logical units if necessary
- a SAN that offers deduplication to reduce redundant data storage, alleviate data bloat, and achieve true single-instance storage where appropriate
- storage hardware that will be increasingly more performance savvy as normalization increases to provide data retrievals quickly.

Software Considerations

SQL Server stores database data in 64KB extents on the hard drive. These extents consist of 8KB pages that hold table row values from the database. Each 8KB page contains page-identifying overhead information and the first/last pages of an extent hold extent overhead. Furthermore, data changes or additions are not even written into these extents until the data is flushed to the database data files from the database transaction log file during a process known as checkpoint. Using write-ahead logging, SQL first writes all new data to a memory buffer, then to the database's transaction log on the hard drive. This write-ahead method can be negatively impacted by caching controllers on the storage device if they are not SQL-aware.

CROSS REFERENCE

For more information on best practices for employing SQL Server Infrastructure and Architecture as a business intelligence solution, visit EMC at **www.emc.com/solutions/application-environment/microsoft/solutions-for-sql-server-business-intelligence.htm**

Deciding to implement virtual SQL Server machines on your network introduces an entirely subordinate yet equally important set of considerations. There are many virtualization applications on the market. Be sure to choose one that allows online management of virtual machines (so you don't have to take your SQL Server down just to change a virtual machine setting), along with providing portability and flexible growth. Centralized virtual machine management tools will also be a must for large enterprises implementing multiple virtual SQL Server machines.

Disaster Recovery

While SQL Server ships out of the box with disaster recovery tools, many of them are limited to traditional backup and restore functionality that can prove time-consuming during a recovery event. Furthermore, open files can be skipped during backups if Microsoft Volume Shadow Copy Services is not utilized. Also, the native backup and restore tools in SQL Server operate at the database level, not table or row. Often, mission-critical data must be recovered at the record level or "brick level" and using only native SQL tools will require an alternative server and row migration utility.

There is also a new trend in our industry to replace backup and restore policies in favor of data replication. The idea being that a second identical copy of the mission-critical data can be quickly flipped over to in the event of failure of the original/primary instance of the data. Given adequate storage space, replication strategies do provide quicker access to point-in-time data values than traditional restore procedures. So be sure to choose a storage platform for SQL Server that can provide granular data replication and secure access to the replicated date.

Where to Start? At the Beginning...

While the many storage platforms and topologies available in today's SQL Server market may seem overwhelming, choosing the right storage for your environment does not have to be a confusing process. Start by determining exactly what data is mission critical and what data is not. Then establish a mission-critical data delivery plan that outlines special caveats for critical information. And last, get help when you need it. SQL Server can be huge; you may need some assistance wrangling it into the enterprise-class RDBMS and OLAP solution that best serves your business information users. For instance EMC Consulting Services offers a wide range of services to assist you with planning, procuring, and implementing your SQL Server solutions. You'll read more about why EMC is a wise helping hand later in this article.

Determining Mission-Critical Data
Contrary to many user cries, not all data is mission critical! Begin any critical data storage plan by identifying exactly which data is critical and which is benign. Your company's federal regulatory overseers or industry standards body may dictate what data is considered critical. A full risk analysis can also be helpful in determining the monetary impact of SQL Server downtime. Once this impact is determined it can be added to the Mission-Critical Data Delivery Plan and Disaster Recovery Plan. Also, consider getting management approval on a formal data retention policy to avoid over-archiving your data. If data is not relevant or required, let it go!

Establishing a Mission-Critical Data Delivery Plan
Any formal mission-critical data delivery plan should begin with a topology justification and storage standards. Remember to choose the best storage your company can afford, preferably a SAN with redundant channels or iSCSI network paths to preclude the network from becoming a data access failure point. And select a SAN with the best features you can afford, such as solid-state hard drives to reduce power consumption and boost data access times or administrative features that allow flexible design of logical units, thin provisioning, and geographically dispersed data replication. A few more things to look for in your choice of SAN storage:

- Supports thousands of physical drives
- Supports multiple 4GB+ disk directors
- Supports multiple channel directors
- Global memory
- Flexible connectivity (Fibre Channel, iSCSI, GB-Ethernet, FICON, etc.)

Getting the Right Help
When it comes to mission-critical SQL databases, the pool of SQL Server information available on the Internet is vast. Keep in mind that because SQL Server can be implemented in so many different configurations for different purposes, finding a single resource with everything you need may be difficult. Many of Microsoft's web resources are positioned for a specific audience or purpose (such as the MSDN library geared toward SQL Developers/Programmers). Often finding a single resource that incorporates all of the SQL Server information you need requires looking beyond Microsoft, such as toward EMC cross references mentioned earlier.

If you find the wealth of resources out there too confusing to weed through on your own, consider hiring a reputable consulting firm with experience in your company's market space. Seek a firm—like EMC—that has a relationship with Microsoft to streamline your troubleshooting or design questions. Ensure your firm has the expertise in your chosen storage platform's capabilities and features. EMC has eleven Microsoft competencies and has been awarded Microsoft Partner of the Year 20 times. Also, leverage documented best practices and validated solutions to deliver predictability. Good examples of these are EMC Proven Solutions, which are supported by proven methodologies, best practices, and industry standards to minimize risk and increase efficiency across your SQL Microsoft lifecycle.

CROSS-REFERENCE
To learn more about working with EMC Consulting Services, visit: **www.emc.com/services**

Wendy Henry is a Microsoft Certified Trainer (MCT) who has been an independent technical trainer, author, and consultant for more than 10 years. She has specialized in Microsoft SQL Server since 1999 and SharePoint since 2005. Wendy is a contributing partner on SharePoint-eLearning.com and frequently teaches and presents at conferences on WSSv3/MOSS2007. She has written a variety of proprietary courseware for leading technical education centers, and has also been called on to edit technical material by national publishers such as McGraw-Hill and Microsoft Official Learning Products. Her technical certifications include Microsoft (MCITP, MCTS, MCSE, MCT), Novell (CNE, CNI), and Cisco (CUSE, CCNA).

TOOL TIME

windowsitpro.com

Server 2008 R2 AD Recycle Bin

Windows Server 2008 R2's Active Directory Recycle Bin lets you restore accidentally deleted Active Directory (AD) objects. To use the Recycle Bin, you must raise your forest functional level to that of Server 2008 R2 rather than just Server 2008, which means you can't use the feature on your old domain controllers.

The Active Directory Recycle Bin is disabled by default. There's currently no GUI console to enable it. For now, you must use PowerShell to enable the Recycle Bin. Enter

```
Import-Module ActiveDirectory
```

to import all the cmdlets to manage AD in PowerShell. Then, enter

```
Enable-ADOptionalFeature
'Recycle Bin Feature' -Scope
ForestOrConfigurationSet -Target
itproconnections.local
```

where *itproconnections.local* is the name of your forest, to enable the Recycle Bin.

You'll get a dialog box that asks if you're sure about enabling the Recycle Bin; click Yes. Note that once you enable the Recycle Bin, you can't disable it.

To test the Recycle Bin's restore capability, let's delete a user object that has the username user1 and the display name User 1, then try to restore it. After the user object is deleted, we need to undelete the user account. Start PowerShell and enter

```
Get-ADObject -Filter {displayName
-eq "user 1"} -IncludeDeleted-
Objects | Restore-ADObject
```

to undelete the account.

Running this command opens a new PowerShell prompt but doesn't show whether the object was restored. You can use Active Directory Users and Computers to verify that the user account was restored.

—Chris Spanougakis, MCT, MVP Directory Services

InstantDoc ID 103167

■ Server 2008
■ Offline Files
■ Process Monitor
■ Scripting

READER TO READER

Offline File Caching Slows Logon and Logoff

I recently noticed excessive offline file caching during logon and logoff on a particular Windows XP domain machine (called PC1) at a customer's Windows Small Business Server (SBS) 2003 site. (Note that you can configure a server's shared folders, or individual files within those shares, as offline files by browsing to the network item in Windows Explorer, right-clicking the item, and selecting Make Available Offline.)

PC1's domain user (called User1) had tons of files stored in her My Documents folder, which was redirected to the SBS server. Recall that redirection of My Documents is a default setup in an SBS 2003 environment. A good reason for redirecting My Documents is so that the server's nightly backup process backs up the folder. (For information about redirecting the My Documents folder, see the Microsoft article "Redirect My Documents folders," at technet.microsoft.com/en-us/library/cc747413.aspx.)

In addition to the redirection, User1's My Documents folder was set as Available Offline. When a network file or folder is available offline, it's cached locally on the PC. So if the server goes down unexpectedly, the user still has access to his or her files. (For information about using the Offline Files feature, see the Microsoft article "How to use offline files in Windows XP" at support.microsoft.com/kb/307853.) It's possible (and in fact desirable) for a local resource (i.e., a folder or file) to be both redirected and available offline at the same time.

The problem occurred when User1 moved to an office down the hall, and another domain user (called User2) was assigned to PC1. Even though User1 was no longer using PC1, her offline file caching continued on the PC. When User2 logged on to PC1 for the first time, his redirected My Documents folder was immediately cached locally on PC1. Because offline file caching synchronization was subsequently processing for two users, logon and logoff times increased noticeably. In addition, periodic backups of the workstation were inordinately large, because PC1 contained offline files for two users.

I thought all I needed to do to stop the previous user's file synchronization was delete the user's domain profile. I logged on to PC1 as Administrator, right-clicked My Computer, selected Properties (which brings up the System Properties window), and selected the Advanced tab. Under User Profiles, I clicked the Settings button,

A good reason for redirecting My Documents is so that the server's nightly backup process backs up the folder.

selected the appropriate user, and clicked Delete. However, even after I deleted the user's profile, offline files were still synchronizing at logon and logoff.

I contacted Microsoft Product Support Services (PSS) for help and was directed

to the article "How to re-initialize the offline files cache and database," at support.microsoft.com/kb/230738. I followed the steps under Method 1 to delete and re-initialize the offline file cache. The way this solution works is that when User1 logs on to the PC again, her offline file cache is rebuilt. So if User2 never logged back on to the machine, his offline files would never recache locally on PC1.


Bret A. Bennett

This approach worked to purge User1's offline file cache (as well as the cache for all other users on PC1). In addition, this solution completely rebuilds the offline file cache structure, which is beneficial in case the cache has become corrupted. I've since discovered another Microsoft article ("Managing the Offline Files Folder: Mobile Computing" at technet.microsoft.com/en-us/library/cc938821.aspx), which provides two alternative solutions, in addition to the one I used. One of these solutions is sure to meet your needs.

The upshot is that after I deleted User1's offline file cache, User2's logon and logoff times were 10 to 20 seconds faster. This solution will work well in your organization when users use offline file caching and move permanently from one primary PC to another primary PC.

—Bret A. Bennett, IT consultant

InstantDoc ID 103168

Managing NTFS Permissions

Eliminating administrative rights is an easy way to prevent viruses, adware, and other annoyances from being installed on your systems. If you're logged on to a computer as an administrator, all the processes you run have full control of the system, which is a huge security risk. For example, if you view a questionable website as an administrator, adware on that site can easily install and infect the computer. If you view the same website as a user, the adware won't have installation rights and therefore will be prevented from installing.

Microsoft provides a free tool called Process Monitor that you can use to manage NTFS permissions. Process Monitor lets you eliminate administrative rights and configure applications to run with the least amount of privileges. I frequently use this tool on my organization's Citrix servers; you can also use it with all Windows Server and workstation OSs.

Process Monitor monitors your computer's registry, as well as the files and folders on your computer, and reports on everything affected by the running processes. The software is the next generation of two Sysinternals programs called Filemon and Regmon. Process Monitor saves time because it lets you monitor your registry and files simultaneously, whereas Filemon and Regmon required individual monitoring. You can download Process Monitor at technet.microsoft.com/en-us/sysinternals/bb896645.aspx.

In order to run applications with the least amount of privileges, you must first understand application permissions. When you install an application, the installation process typically creates a folder in the Program Files directory and adds some registry entries for the application. Many applications require that you have full access to the application files and registry entries to be able to run the software. In general, the Users group has read-only access to application folders and registry keys—which is why you often get an error message when you try to run an application as a user. An easy way to tell if you're running into a permission problem is to run the application as both a user and an administrator. If the program runs under administrator but not user, a permission issue exists. You can solve most permission problems by modifying the NTFS permissions on your files, folders, and registry keys.

Some applications require low-level kernel and hardware access and are difficult if not impossible to run as a user. If you use Process Monitor to resolve all the permission issues it finds and still can't run an application as a user, you might need to check with the software vendor to determine if any other options exist.

Incorrect NTFS permissions can have a negative effect on your OS and applications. For example, incorrect permissions can loosen your security, and incorrect registry entries can cripple a machine. Don't give too much access to the Users group. Users shouldn't have full control of the Windows folder or any other root or system levels of the Windows file structure and registry. For security reasons, it's best to grant access on a folder by folder or registry key by registry key basis.

Process Monitor takes out all the guesswork and shows you exactly where a denial of access is occurring, by individual file, folder, or registry key. Before you run Process Monitor, be sure to take a complete system backup. In addition, you might want to test this procedure on a test machine before applying it in a production environment.

To use Process Monitor to manage your NTFS permissions, follow these steps:

1. Start Process Monitor; it will start capturing events automatically.
2. Log on as a user, and open the application you want to manage.
3. When the application fails to run or generates an error, stop the capture.
4. Within Process Monitor, perform an Access Denied search. The search results will show the files, folders, and registry keys that are being denied access.
5. Right-click the item that's being denied, and select Jump To. This action will open the corresponding folder or registry key.
6. Right-click the file, folder, or registry key being denied; then, select Properties, open the Security tab, and set the NTFS permissions to give the Users group full access. If the Users group doesn't exist, add it and configure it for full access.
7. Repeat Steps 4 through 6 to adjust the permissions for each Access Denied item that Process Monitor found.
8. Test each application while still logged on as a user. If the permission problem is resolved, the application will run correctly. If the application still won't run, repeat Steps 1 through 6.

In addition to troubleshooting permissions, I use Process Monitor to find the files and registry entries that a particular piece of software is using. The tool is useful in helping determine a file's location. For example, I've used Process Monitor to locate reports that were running in the background of my company's accounting software. Without this tool, I would have

had to go through more than a hundred reports to determine which one needed to be updated.

—Chris Betlach, IT manager

InstantDoc ID 103169

Chris Betlach

Making a Logon Script Expire

Sometimes it's useful to have a standard network script perform an additional ad-hoc task for a few days. Although configuring this task isn't difficult, it isn't obvious how to make the solution work consistently if you aren't familiar with the ins and outs of the scripting language. To demonstrate such a solution, I'll use a couple of lines of VBScript to prevent code from executing after a specific date.

Although you can use this approach for anything you need to expire, user printer mappings provide a good example of why such functionality is useful. Since printer-mapping data is available only in the user context, gathering such data is easiest from a logon script. You can simply add printer enumeration code to a logon script, then send the data to an available logon server with the WScript.Shell LogEvent method.

Performing such an audit from a logon script presents a couple of problems.

The stop date should be the day after the last day you want the code to run.

First, you might capture only a fraction of users if you run the code for only part of a day—or even a full day. Depending on the nature of the network, you might need several days or even a couple of weeks to obtain information about a majority of users. Second, because the code runs at every logon, you'll get the same data repeatedly for users who log on frequently; eventually, you'll want to stop putting all this data into the event logs.

In an ideal world, you'd remember to go back and remove the code from the logon script after a week or so. However, snags tend to occur, particularly if you're performing the audit as part of offsite technical support or if you aren't the only technical support person working with the network. Having a technique for skipping code after a particular date is a small bit of insurance that helps limit the effect of your audit.

To make code expire within a script, insert a line of code that checks the current date and runs the subsequent code only if the date is before a particular stop date. Keep in mind that you might run into problems with how VBScript handles dates. VBScript is very flexible about not only what it recognizes as a date but also how it converts the information to a date. This means that your off-the-cuff date used in a script written under the assumption of U.S. dating format might be misinterpreted elsewhere. Depending on the date specified, the code might never run at logon for a British or ISO localized computer—or it might run during logon for months or years.

There are multiple ways to ensure that VBScript interprets a hard-coded date correctly, but one method stands out as being both simple and reliable: Specify the date in the format yyyy-MM-dd, where yyyy is the 4-digit year, MM is the 2-digit month, and dd is the 2-digit day. Given 4 initial digits and separating dashes, VBScript will always interpret this as a standard ISO 8601 date—including the one possible edge case, in which a system displays dates using the format yyyy-dd-MM (which to my knowledge isn't used anywhere in the world).

Using the yyyy-MM-dd approach, you'd specify February 1, 2010, as 2010-02-01. To convert this information into a date instead of merely a string that looks like a date, I use VBScript's # mark instead of quotes when specifying the date in a script. With an unambiguously interpreted date, all you need to do is check the current system date and compare it to the stop date. You can use an if-then loop with the date test to force the code to run only until the stopping date, like so:

```
If Date < #2010-02-01# Then
   ' Code goes here
End If
```

One thing you should be aware of is that the stop date you specify should be the day after the last day you want the code to run. In VBScript, a date is more accurately a date and a time. When you call VBScript's Date() method, although it might be displayed as simply a specific date, the actual date inside VBScript includes a time of day. Therefore, 2 A.M. on February 1, 2010, is a larger date value than just February 1, 2010. Although you could extend the code to deal with time, doing so adds more potential ambiguities. In addition, specifying a time still doesn't give you any guarantees, because the date is interpreted locally. So, for example, for whatever stop date you specify, a system on London time will skip the code 10 hours before a system on Honolulu time will do so. If you need a more complex solution, I suggest performing searches on the Windows Management Instrumentation (WMI) wbemDateTime class.

The code that Web Listing 1 contains (www.windowsitpro.com, InstantDoc ID 103170) demonstrates a usable date-expiring chunk of code that audits user printers and sends them to the logon server with the name of the user and the computer from which they were logging on. Data will show up in the Application log, with the source shown as WSH. As written, you can insert the code at the end of a logon script and it will work until February 1, 2010; from that date on, WSH will skip the code chunk. It's possible to use this code as is for printer auditing; just remember to change the date from #2010-02-01#. You still need to clean up the logon script after you finish auditing, but using a date test makes the post-audit problem a simple matter of cleaning up already-dead code, rather than deleting a lot of unnecessary logging.

Alex K. Angelopoulos

—Alex K. Angelopoulos, IT consultant

InstantDoc ID 103170

- Active Directory
- Windows Storage Server
- Outlook
- Windows 7
- File Servers
- IIS 7.0

ANSWERS TO YOUR QUESTIONS

Q: I downloaded Windows Storage Server 2008 from Microsoft, but I wasn't prompted for an Administrator password when I installed it. What's the password for Administrator?

A: This is one of those annoying times you need to read the documentation. The Release Notes (WSS2008_RELNOTES.DOC) on the Windows Storage Server 2008 embedded tools CD (the tools CD, not the installation media) tell you the password is wSS2008!. You can change the default password by creating an Unattend.xml file.

—John Savill

InstantDoc ID 102972

Q: Is there a way for Windows Server 2008 and above to export and compare Active Directory schemas?

A: It's very common for companies to have multiple forests that they need to merge, but before they're merged, IT staff needs to know if there are differences in the schema configurations of the two forests. Fortunately, you're able to export the schema configuration (which is common for all domains in a single forest) using the ldifde command, as shown below. Note that you pass the forest root domain in the command.

```
C:\>ldifde -f SavSchema.ldif -d CN=
Schema,CN=Configuration,DC=Savillte
ch, DC=Net
Connecting to "SAVDALDC11.
savilltech.net"
Logging in as current user using
SSPI
Exporting directory to file SavSche-
ma.ldif
Searching for entries...
Writing out entries.................
....................................
....................................
........................
1550 entries exported

The command has completed success-
fully
```

You can now use this file to compare your schema with another schema output or a live schema using various third party tools or the Active Directory Schema Analyzer utility. If you install the Active Directory Lightweight Directory Services (AD LDS) role in Server 2008, the AD Schema Analyzer (ADSchemaAnalyzer.exe) is also installed. You can run Schema Analyzer using a link in the Advanced Tools section of Server Manager, or you can run it directly as C:\Windows\ADAM\ADSchemaAnalyzer.exe. You don't have to create any AD LDS instances—you just need to install the role to get access to the tools.

Once you've executed the tool, you have the option to load a target schema and a base schema. For both the target and base, you can load either an LDIF file, as shown here, or the schema from a live AD (by passing a DC and credentials). This means you can compare a live AD to an LDIF file, compare two LDIF files, or compare two live Ads.

Once both schemas are loaded, the utility compares them. You can select the "Hide present elements" option to show only differences between the schemas. You can select each element you want to export individually, or include every element using the "Mark all non-present elements as included" option from the Schema menu.

To create a file containing the differences between the schemas, select "Create LDIF file" from the File menu. You can load this file into another forest to close any differences. If you open the difference file, you'll see text similar to the following:

```
# Attribute: accountExpires
dn: cn=Account-Expires,cn=Schema,cn=
Configuration,dc=X
changetype: add
objectClass: attributeSchema
attributeId: 1.2.840.113556.1.4.159
```

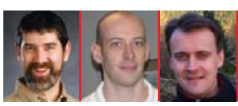
Note that for the domain, it only has dc=X. To load the differencing file you need a valid domain, but you don't have to edit the difference file—you can tell the ldifde utility to make the change.

To import, use the command below. Note the switch -c, which tells the command to replace dc=X with the DC=Savilltech,DC=Net. The -I tells it to import.

```
ldifde -I -f difference.ldf -c dc=X
DC=Savilltech,DC=Net
```

—John Savill

InstantDoc ID 102958



William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Jan De Clercq | jan.declercq@hp.com

Q: What is Outlook 2007 with BCM?

A: Business Contact Manager (BCM) is a Microsoft Office 2007 add-on available in the Small Business, Professional, and Ultimate versions of Office 2007. It can also be purchased as a separate product. It's aimed at small companies of about 25 users or fewer, but larger companies can certainly use it where only a small group of users needs access to a customer relationship management (CRM) application. If the company requires more than 25 users, then an enterprise-level solution should be employed.

BCM integrates with the Outlook user experience and shows the potential of using Microsoft Outlook as a development platform for business intelligence (BI) applications with the ability to access and present data in a useful manner. BCM has its own drop down menu options and a placeholder in the folder view that renders customer, account, and project data from a SQL database.

BCM doesn't use Exchange resources or an Outlook PST to store data—it requires SQL Server 2005 Express edition. This can be installed locally or on a remote, shared location. Interestingly, PST files aren't supported across the LAN for reasons outlined in the Microsoft knowledge base article 297019, but SQL Server is made for that purpose. BCM for Office Outlook 2003 used Microsoft SQL Desktop Edition (MSDE). SQL Server 2005 Express has compatibility problems with beta and RC versions of Windows 7. You must install SQL Server 2005 Express separately and apply SQL Server 2005 SP3 before running SQL Server 2005. When installing on Windows 7 RTM, SQL Server will prompt the installer about this requirement.

BCM was also available with Outlook 2003, but lacked many features typically found in basic CRM applications. Many of these deficiencies were addressed in BCM 2007. Performance remains a problem on weaker hardware, as it was in Outlook 2003. I'd consider the system requirements outlined on the 2007 Microsoft Office system requirements site (an additional 500MB of RAM and 500MB of drive space just for BCM, over and above Office or Outlook) as the bare minimum. The SQL database adds to resource consumption and competes for disk I/O, memory, and CPU cycles. Limiting the amount of memory allotted to SQL and using multiple hard drives to split read/write activity can help ensure that the workstation doesn't get overwhelmed serving SQL processes.

BCM continues with Office Outlook 2010 and has many improvements, such as an improved, gadget-driven dashboard, to compete with more formal customer relationship management applications.

—William Lefkovics

InstantDoc ID 102862

Q: I have a hung process in Windows 7 or Windows Server 2008 R2. Is there an easy way to tell why it may be hanging?

A: The Windows 7 version of RESMON has a neat capability that performs an analysis of the processes wait chain and attempts to tell you what the process may be waiting on, which may identify why it has hung. Right-click the process and select Analyze Wait Chain... from the context menu.

Once the command is executed, an analysis is performed and the wait chain is displayed, as shown in Figure 1. In my case, there were threads waiting on network I/O.

— John Savill

InstantDoc ID 103080

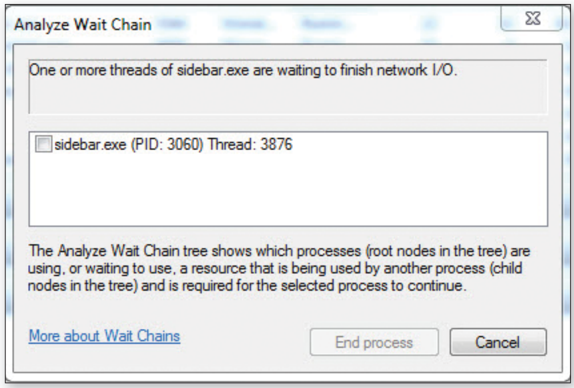


Figure 1: Results of the processes wait chain analysis

Q: I want to install an enterprise certification authority (CA) on one of my Active Directory (AD) domain controllers (DCs). Even though I'm logged on as a domain administrator, the option to install the CA as an Enterprise CA is greyed out in the installation wizard—it only lets me install a Standalone CA. What's wrong here, and how can I resolve this?

A: The problem is that you don't have sufficient privileges for writing the Enterprise CA configuration information in AD. To remedy this, make sure that the account you use to install the Enterprise CA is a member of built-in Enterprise Admins group. For more information on the exact difference between Enterprise and Standalone CAs, see the Microsoft Technet article at tinyurl .com/ya8dscc.

—Jan De Clercq

InstantDoc ID 103010

Q: How can I make Outlook 2007 open directly to my To-Do List?

A: On my desktop, Microsoft Office Outlook 2007 remains open for days, even weeks at a time. But some users close and re-open Outlook many times a day, or at the very least they close it at when they log off at the end of the day. In the morning, those users may have a preference as to which folder is opened first when they launch Outlook. Whether you launch Outlook from the Start Menu, a desktop shortcut, or the quick launch menu, Outlook opens to a default folder. This is typically the Inbox, where users spend most of their time in Outlook. However, you can choose to have Outlook open to a different folder.

As an example, I'll change the folder Outlook opens when it's launched to the To-Do List. By opening the To-Do List first, users can review their tasks before moving on to the messages in their Inbox. Choosing to open Outlook to the To-Do List makes sense for workers who don't use email, but need access to tasks.

To make this change from within Outlook, go to Tools, Options, and select the Other tab. Then click the Advanced button under the General section. In the Advanced Options window, there's a Browse button for the option Start in this folder.

This is the same setting in Microsoft Office Outlook 2003, but Outlook 2007 adds the option to open to the To-Do List. After selecting the To-Do List, close Outlook, ensuring the outlook.exe process terminates. When you restart Outlook, it'll open to your To-Do List. For some, this may be a better place to start the day.

The To-Do List is really a view of the Task folder and can be shown in the To-Do Bar in Outlook 2007 for a limited number of tasks. For information on customizing the To-Do Bar, see my article, "How do I configure views in Microsoft Office Outlook 2007's To-Do Bar using either menu commands or the registry," InstantDoc ID 98436.

You can have Outlook start in any folder in the folder list, including user-created folders or sub-folders. For Outlook 2002 or earlier, you create a new shortcut to outlook.exe with the /select startup switch. For example, to start Office Outlook 2002 or earlier in the Calendar folder, you'd create a new shortcut with the following:

```
"C:\Program Files\Microsoft
Office\Office10\Outlook.exe" /select
outlook:Calendar
```

—William Lefkovics

InstantDoc ID 102861

Q: How can I stress test my file server and figure out how many users it can support?

A: Microsoft will soon offer the new File Server Capacity Tool (FSCT) for this purpose. As of October, it's already available as a release candidate at connect.microsoft.com.

The tool isn't a planning tool—those would typically let you say how many users, shares, and so on you need to support and then generate a server specification. This tool runs on your file server and stresses it with emulated workloads, then tells you what capacity the file server can support in terms of maximum users, throughput, and response time, and tells you where the bottlenecks are. FSCT is a command line utility without a GUI, so it's very much targeted at IT professionals and solution providers.

To use the tool, you need the server that's being tested, a client computer, and a computer acting as the controller. Ideally, you want many client computers, to ensure you're really taxing the server—Microsoft has performed testing with up to 120 clients. You also need an extra network that's used between the clients and the controller computer to coordinate all the file server requests. Because you need this extra network, each client requires two NICs, one connected to the normal network to make requests to the server and the other connected to the controller network. The controller traffic uses ports 5000 and 5001.

FSCT uses "scenarios" for testing. Scenarios are sets of actions that each client will perform. They're defined in XML files and implemented via a DLL. Microsoft provides a single scenario with FSCT, but vendors can create new ones for their products.

You need to install FSCT on all machines that are part of the test, including the server, controller, and clients. The FSCT download includes detailed documentation that provides the commands that need to be run on the controller, server, and clients. The commands follow this structure:

1. Run the FSCT prepare server command on the server with the required parameters, which include the clients, password, simulated number of users, and the scenario.
2. Run the FSCT prepare controller command on the controller.
3. Run the FSCT prepare client command on the clients.
4. Run the FSCT run client command on the clients.
5. Run the FSCT run controller command on the controller.

Once all the tests have run, run the FSCT cleanup command on the server, controller and clients.

A text file is created once the testing is completed that you can examine to get the output of the capacity test. The file shows when the server became overloaded and other performance metrics. The test also creates a more detailed XML report, and you can import and manipulate the XML report with other tools.

To summarize, FSCT is a great tool, but it requires a significant amount of infrastructure and planning to get running. It allows you to get very good information about the capabilities of a file server. The network card requirements may seem like a hindrance, but if you virtualize the clients and the coordinator, it's really not a big deal to create two virtual network interfaces and a local network at the virtualization layer for the coordinator traffic.

—John Savill

InstantDoc ID 103065

Q: Is certificate mapping still around in IIS 7.0?

A: To facilitate web server access control management, IIS 6.0 allows administrators to map IIS client certificates to Windows accounts—a feature called certificate mapping. You can use certificate mapping to apply resource permissions defined for Windows accounts to users that authenticated to your IIS web server using an SSL client certificate.

Certificate mapping is still supported in IIS 7.0, but it isn't exposed in the IIS 7.0 GUI. To define certificate mappings, you must edit the IIS 7.0 configuration files, which is a lot of work. Instructions are available at tinyurl.com/ycdwfet.

The good news is that Microsoft recently released a client certificates plug-in for IIS 7.0 that administrators can use to define certificate mappings from the IIS 7.0 management GUI. You can find a download of x86 and x64 versions of the plug-in, along with screenshots and other useful information, on the MSDN blog at tinyurl.com/y8ac8pk.

—Jan De Clercq

InstantDoc ID 103011

Q: How do I add additional remote sources to Windows 7's search using search federation?

A: Windows 7 makes it easy to search locations on the Internet using Explorer through the new Search Federation feature. Many sites provide ODSX files that can be downloaded and executed to add a new option to the Users, Search

area. After you double-click the OSDX file, you'll be prompted to install it, as shown in Figure 2.

I've provided OSDX files for Amazon.com, Bing, Channel 9, TechNet Edge, and YouTube in a zip file at the online version of this article. Got to windowsitpro.com and go to InstantDoc ID 103042 to download them.

Once you've installed the ODSX file, just type in a search, and the results are found from the selected site. Note that the results will vary based on the site being searched. Some sites return results, comments, and thumbnails while others will return only some of this data. An example execution for YouTube is shown in Figure 3.

You can create your own ODSX files, as long as the site you want to search provides an RSS search feature. Below is an example format—replace the red locations with actual RSS search locations to make it work.

```
<?xml version="1.0"
encoding="UTF-8"?>
<OpenSearchDescription
xmlns="http://a9.com/-/spec/
opensearch/1.1/" xmlns:ms-
ose="http://schemas.microsoft.com/
opensearchext/2009/">
<ShortName>NT FAQ</ShortName>
<Description>Search NTFAQ.COM via
Windows 7 Search.</Description>
<Url type="application/rss+xml"
template="http://www.ntfaq.com/searc
h?q={searchTerms}&amp;format=rss"/>
<Url type="text/html"
template="http://www.ntfaq.com/
search?q={searchTerms}"/></
OpenSearchDescription>
```

—John Savill

InstantDoc ID 103042

Q: What options does Windows provide to attach automated actions, such as sending an email alert message, to events on a Windows machine?

A: In the Event Viewer that Microsoft includes in Windows Vista, Windows Server 2008, and later OSs, you can easily attach an action to the occurrence of a particular event. When you create an action from the Event Viewer, Windows automatically creates the associated task in the Windows Task Scheduler.

To create an event-triggered action from Event Viewer, select Attach Task to this Event… in an event's context menu or the associated task in the Actions pane. Selecting this option will open the Create Basic Task Wizard. In the wizard, you can select one of three notification actions (Start a program, Send an e-mail, or Display a message) that will be executed when a particular event occurs.

After you've successfully created the event-triggered action, a dialog box appears to inform you that a task has been added to Task Scheduler. From then on, you must use Task Scheduler to edit, disable, or delete the event-triggered action.

Windows XP and Windows Server 2003 also support event triggers, but the functionality isn't integrated in the OS as nicely as it is in Vista, and these OSs require additional tools. Microsoft provides a tool called eventtriggers.exe in XP and Server 2003 that lets you define event-triggered actions from the command line. See tinyurl.com/yeo3hcd for more information on Eventriggers.exe.

Eventtriggers.exe requires you to use other programs if you want to automate certain actions. For example, if you want eventtriggers.exe to send an email message from the command line, you must use another tool, such as the Blat freeware tool, available at www.blat.net.

—Jan De Clercq

InstantDoc ID 103012

Q: How can I open a command prompt at my current location in the Windows 7 Explorer?

A: In previous versions of Windows, you could install an application to enable a "Command Prompt Here" context menu item in Explorer via a registry setting. With Windows 7, this functionality is built into the OS. Just hold down the Shift key as you right-click in Explorer and you'll see an "Open command window here" option that will open a command prompt for the selected folder.

—John Savill

InstantDoc ID 103040

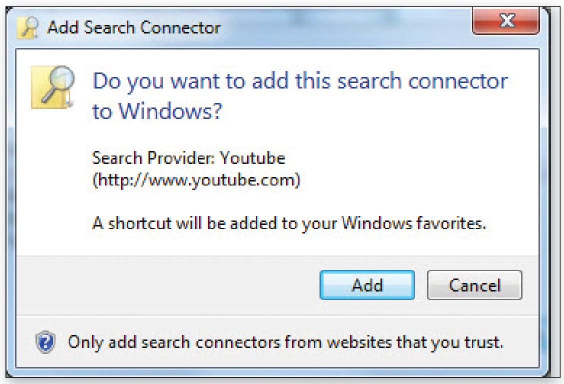


Figure 2: Prompt for adding a search provider

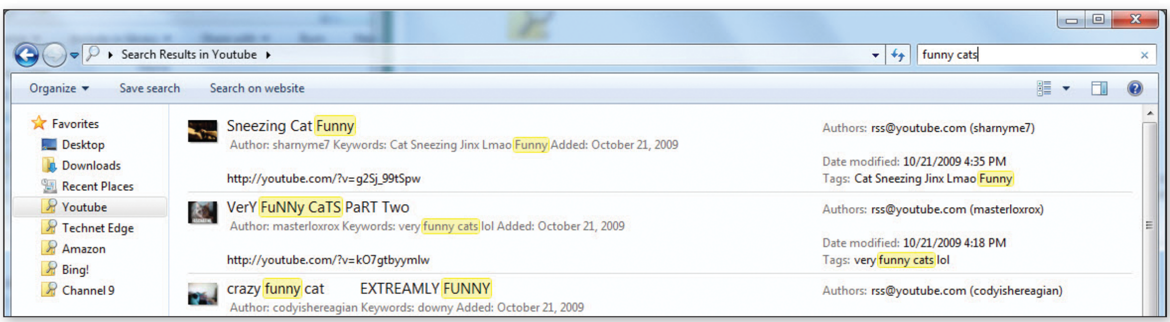


Figure 3: Example results using YouTube as the search provider.

UPGRADING FROM WINDOWS XP TO WINDOWS 7

by Michael Otey

Discover Microsoft's Best OS Yet

Most businesses are still running Windows XP—but with Windows 7 now available, many companies are weighing the costs and benefits of upgrading from XP to Windows 7. XP is a well-known commodity; it's stable, but it has also grown a bit long in the tooth since its release back in 2001. Windows 7 offers many enhancements over XP both from a usability perspective and in the areas of security and manageability. For more information about the new features, see "Windows 7 in the Enterprise" (June 2009, InstantDoc ID 101885).

Unfortunately, the path from XP to Windows 7 isn't a smooth one. Although XP users qualify for upgrade licensing, there's no in-place upgrade from XP to Windows 7. The only way to upgrade in-place is to go from XP to Windows Vista, then from Vista to Windows 7. This is a time-consuming and risky process that few users want to attempt.

The best way to move from XP to Windows 7 is to buy a new system with Windows 7 preinstalled. Today's multi-core systems are significantly more powerful than the desktop systems built a few years ago. Replacing both the hardware and the OS would provide the best results in the long run. However, not all businesses are ready to replace their desktops with new systems—even though the economy appears to be turning.

Upgrade Process

Although installing Windows 7 on an older XP system is possible, there are difficulties and limitations with this approach. In fact, because there's no in-place upgrade from XP to Windows 7, the upgrade process might be more aptly termed a migration. The general process for moving from XP to Windows 7 is:

1. Select an edition of Windows 7.
2. Verify your system's Windows 7 compatibility.
3. Use Windows Easy Transfer to migrate your XP data and settings.
4. Install Windows 7.
5. Restore your data and settings.
6. Reinstall your applications.

Table 1: Windows 7 Retail Pricing

Windows 7 Edition	Windows XP Upgrade License	Windows XP Full License
Windows 7 Starter	N/A	N/A
Windows 7 Home Basic	N/A	N/A
Windows 7 Home Premium	N/A ($119.99 Vista only)	$199.99
Windows 7 Professional	$199.99	$299.99
Windows 7 Enterprise	N/A	N/A
Windows 7 Ultimate	$219.99	$319.99

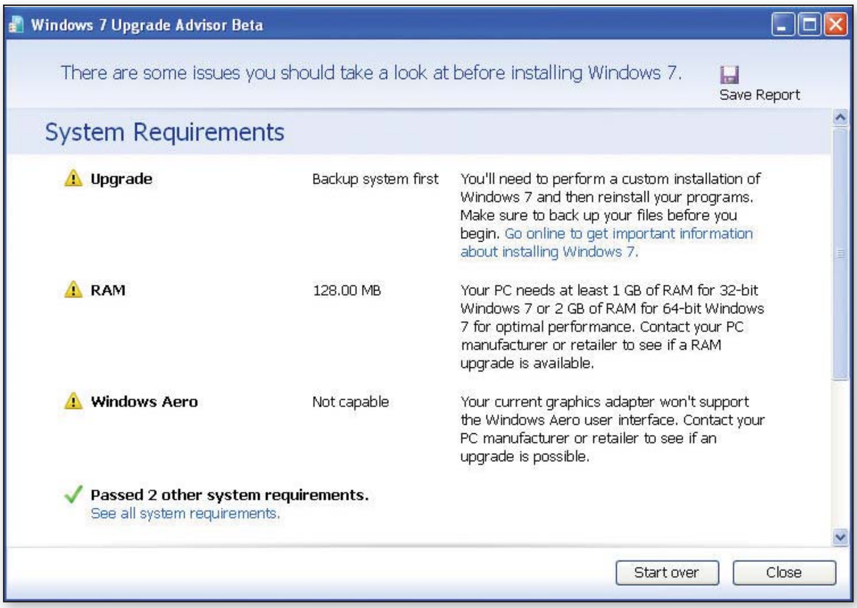


Figure 1: Windows 7 Upgrade Advisor results window

Figure 2: Selecting a transfer method in the Windows Easy Transfer wizard

Selecting a Windows 7 Edition

The first issue to address is whether you want to upgrade to the 32-bit or 64-bit edition of Windows 7. This decision mainly depends on the processor capability of the system being upgraded. Most new systems have 64-bit processors, but many older systems don't. (If you're not sure whether your system is 64-bit capable, download and run the SecurAble utility from www.grc.com/securable.htm.) Even if the system to upgrade is 64-bit capable, you'll really only benefit from the 64-bit edition of Windows 7 if you plan to use more than 4GB of RAM in the system. Moving from 32-bit to 64-bit as part of the upgrade could also result in device compatibility issues because there are more 32-bit device drivers than 64-bit device drivers. The bottom line is that if your system is already running 64-bit XP, go ahead and upgrade to 64-bit Windows 7. If the system is 32-bit, as most XP systems are, then you're probably better off upgrading to 32-bit Windows 7. The exception to this is the rare case in which the hardware is 64-bit capable and you need more than 4GB of RAM.

After you've made the decision as to which CPU platform to use, you need to consider two additional upgrade aspects: upgrading your Windows license and upgrading the OS itself. Microsoft provides all XP users with a reduced upgrade license cost. Table 1 lists the retail costs for Windows 7 editions.

Most business users will want Windows 7 Professional, Enterprise, or Ultimate, all of which support joining a domain and management using Group Policy—unlike the Starter and Home editions. With essential features such as BitLocker and AppLocker, the Enterprise Edition is the most desirable—but it's limited to Software Assurance (SA) customers. If you want these Windows 7 features and you're not an SA customer, you'll need to upgrade to Windows 7 Ultimate.

Verifying Windows 7 Compatibility

It's important to remember that Windows 7 is essentially the next release of Vista. It shares most of Vista's core attributes, including the Aero interface, a new device driver model, and User Account Control (UAC). One of the reasons that Windows 7 has received better acceptance than

Vista is the fact that there has simply been more time for Microsoft and third parties to address the main customer complaints about Vista. For example, Microsoft refined UAC to reduce the number of notifications, and performance-tuned Windows 7 for the tasks customers commonly perform, thereby making the OS more responsive. In addition, third-party hardware vendors have had an additional three years to develop Vista- and Windows 7-compatible device drivers, which reduces the problem of incompatible hardware.

When evaluating your XP system's hardware platform in preparation for upgrading, it's important to remember that Windows 7 has higher system requirements than XP. The minimum Windows 7 system requirements are:

- 1GHz or faster 32-bit (x86) or 64-bit (x64) processor
- 1GB of RAM (32-bit) or 2GB of RAM (64-bit); additional 1GB of RAM for Windows XP Mode (XPM)
- 16GB of available hard disk space (32-bit) or 20GB (64-bit)
- DirectX 9 graphics device with Windows Display Driver Model (WDDM) 1.0 or higher driver
- 128MB of video memory for the Aero interface

Keep in mind these are Microsoft's *minimum* requirements—you'll get a much better experience running a multi-core system with 2GB of RAM or more. Many existing XP systems meet the minimum requirements, other than the graphics support. Many older systems, especially those with integrated graphics adapters, don't meet the Windows 7 Aero interface requirements. However, this doesn't mean these systems won't run Windows 7, because Aero support isn't required. You can run Windows 7 using the Windows 7 Basic or Classic themes; you just won't have the catchy Aero features, such as transparent windows. However, Aero might not be vital to some XP users because XP doesn't have this feature either. To take advantage of Aero on XP, you can perform a graphics upgrade.

If the XP system you're upgrading meets the minimum system requirements, the next step is to run the Windows 7 Upgrade Advisor, which scans your system's devices and applications to see whether they're compatible with Windows 7. The Windows 7 Upgrade Advisor runs on Windows 7, Vista, or XP SP2 and requires the .NET Framework 2.0. You can download the Windows 7 Upgrade Advisor from www.microsoft.com/windows/windows-7/get/upgrade-advisor.aspx.

To start your Windows 7 installation, first install the Windows 7 Upgrade Advisor on the XP system you want to migrate. The installation process takes just a few seconds. Then, run the Windows 7 Upgrade Advisor from the Start menu. After the Windows 7 Upgrade Advisor starts, you need to select the option to scan your system. The scanning process takes several minutes; when it's finished you'll see a results window similar to the one in Figure 1.

Windows 7 is essentially the next release of Vista; it shares most of Vista's core attributes, including the Aero interface, a new device driver model, and UAC.

The Windows 7 Upgrade Advisor flags serious upgrade issues with a red X. Warnings are marked with a yellow triangle, and a green check mark shows requirements that passed. For example, in Figure 1 the system will require a RAM upgrade before the Windows 7 upgrade. Although you should consider the cause of warning errors, you need to realize that they won't prevent the upgrade. Nevertheless, if the Windows 7 Upgrade Advisor points out an issue, you should evaluate and resolve the problem if necessary before proceeding with the upgrade.

Using Windows Easy Transfer

Once you've made sure that the XP system meets the requirements for upgrading to Windows 7, you're ready to begin the upgrade process. Although you can't transfer your existing XP programs to Windows 7, you can use the Windows Easy Transfer tool to transfer your desktop data and settings.

Windows Easy Transfer for XP can move Windows data and settings from a 32-bit version of XP to either a 32-bit or 64-bit version of Windows 7. It can also move data and settings from a 64-bit version of XP to a 64-bit version of Windows 7, but it can't move from a 64-bit version of XP to a 32-bit version of Windows 7. Windows Easy Transfer is available in 32-bit and 64-bit versions from windows.microsoft.com/en-us/windows7/products/features/windows-easy-transfer.

You need to install the Windows Easy Transfer wizard on your XP system before beginning the Windows 7 setup process. Installation is simple and takes only a few seconds. After setup is complete, you can run the wizard from the Start menu. Clicking through the Windows Easy Transfer welcome screen takes you to the screen in Figure 2, where you can select a transfer method.

If you're migrating to a new computer, select either *An Easy Transfer cable* or *A network*. An easy transfer cable is essentially a USB cable that connects two computers. A network uses your existing network for the XP-to-Windows 7 link. However, both of these options require the Windows 7 system to be available on the network—which isn't the case if you're upgrading an existing system. For an upgrade, use the third option: *An external hard disk or USB flash drive.*

Windows Easy Transfer will save your current data and settings to a file. After you select a transfer option, Windows Easy Transfer will analyze your system for items to transfer and will estimate the size of the transfer. Most XP systems will contain a lot of data. Although the data is compressed, the size could easily be hundreds of gigabytes. Remember that if you're upgrading an existing system you don't need to transfer your data because it will already be there. If you just want to transfer your settings, select the check box next to your user profile and click Next.

You'll need to provide a password for the file. Select the Save As option to select a location for the file. The dialog box will indicate that you should save the file to a USB key or a network drive, but you can actually save it anywhere, including the local drive. If

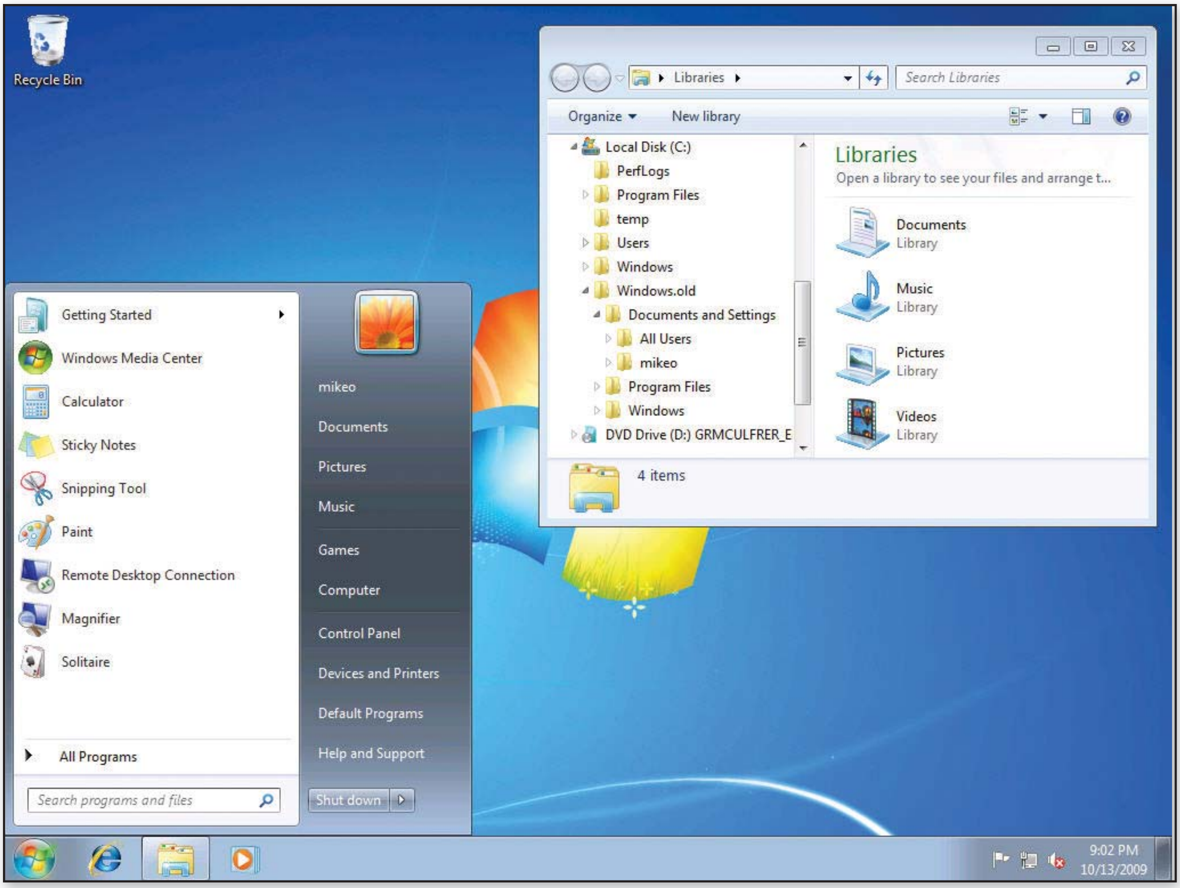


Figure 3: Newly installed Windows 7 desktop

you're performing an upgrade of an existing system, the local drive is the best place to store the file—if there is adequate disk space. Saving the settings and files takes a few seconds to several minutes depending on the amount of data and the storage location you select. By default, Windows Easy Transfer saves the data and settings in a file named *Windows Easy Transfer - Items from old computer.MIG.*

As cheap insurance you might consider purchasing an additional hard drive and performing a clean installation of Windows 7 on that drive, to leave your existing XP installation and files intact. However, don't be misled into thinking that you'll have a dual-boot system. Although there are ways to create a dual-boot XP and Windows 7 system when installing Windows 7, it's more involved than just installing Windows 7 on a new hard drive. (For information about dual booting Windows 7 with an existing OS, see "How do I dual boot an existing OS with Windows 7 or Windows Server 2008 R2 installed in a virtual hard disk [VHD] file?" InstantDoc ID 101457.)

Windows 7 Clean Installation

To start the Windows 7 installation process, insert the Windows 7 installation media on a system that's running XP. The installation process lets you choose between *Checking compatibility online* and *Install now.* Since you've already run the Windows 7 Upgrade Advisor and resolved any issues that would thwart the installation process, select *Install now.* The Windows 7 setup program will install the required setup files on the XP system and will display the *Get important updates for installation* screen. Although the default option is *Go online to get the latest updates for installation (recommended),* selecting *Do not get the latest updates for installation* is a faster option. You must also agree to the EULA.

Next, you must specify either custom installation or upgrade. Note that the upgrade option doesn't work, although you can select it. To install Windows 7 on your XP system, select *Custom (advanced).* Choosing this option starts a clean installation of Windows 7.

The setup program then displays the available partitions on the system and asks you for the partition on which to load Windows 7. Select the appropriate disk partition and click Next. If the partition contains your XP system files, the setup program creates a Windows.old directory and moves your existing Windows directory into it. Your system's Program Files directory is also saved in the Windows.old directory, but you won't be able to use your XP programs from your Windows 7 installation. The Custom option copies the Windows 7 binary files to the selected partition.

From this point on, follow the standard Windows 7 setup procedure. Select the country, language, and keyboard layout. Provide a user account name and computer name, as well as a password and password hint for the user account. Enter your Windows product key when prompted. Select the method you want to use for Windows Update. (The default is *Use recommended settings,* which automatically downloads and installs updates every day at 3:00 A.M.) Next, select your time zone and set the system clock if necessary. Finally, select

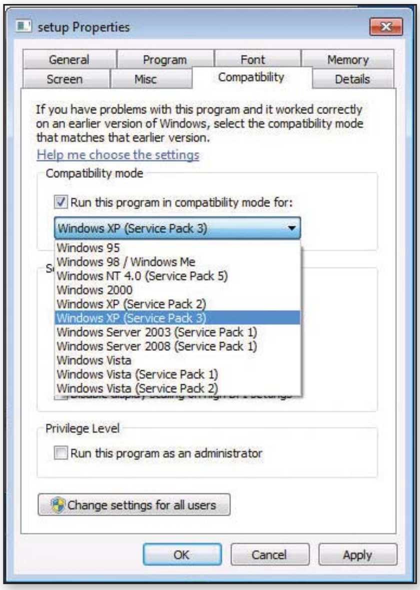


Figure 4: Windows 7 application compatibility properties

the type of network you're connected to—home, work, or public. If you're upgrading an XP business system, you'll typically want to select the *Work network* option. If you're upgrading a personal system that you use at home, you'll want to select the *Home network* option.

After setup completes, you'll see the Windows 7 desktop that Figure 3 shows. Note the new Windows 7 taskbar at the bottom of the screen. In the upper right half of the screen you can see Windows 7 Explorer, with the new Libraries feature. The adjacent treeview shows the Windows.old directory, with its Documents and Settings, Program Files, and Windows subdirectories. This is where the setup program saved your XP system files and applications.

Restoring Data and Settings

After Windows 7 is installed, you need to restore the XP data and settings that you used Windows Easy Transfer to save earlier. This step doesn't require any installation on the Windows 7 system. Simply open Windows Explorer, navigate to the directory where you saved your Windows Easy Transfer file, and double-click the file. Windows 7 will automatically start the Windows Easy Transfer program and prompt you for the password for the Windows Easy Transfer file. You must then select the items you want to transfer. After your XP data and settings are restored, you'll need to reboot. The reboot will restore your desktop and other user profile settings from the XP system. This step completes the migration, and you can move on to reinstalling your programs.

Reinstalling Programs

Because there's no in-place upgrade, moving your programs to Windows 7 requires reinstallation. Be sure to have your installation media handy, as well as the installation keys or activation codes for each application that you want to reinstall. Microsoft provides absolutely no help for reinstalling programs, but you can use a third-party product such as Laplink Software's PCmover (www.laplink.com/pcmover) to transfer programs and applications between systems.

Before installing your applications, check each vendor's website to verify Vista or Windows 7 compatibility. Not all vendors list Windows 7—but most Vista-compatible programs also run on Windows 7. For specific information about program compatibility, see Microsoft's Windows 7 Compatibility Center (www.microsoft.com/windows/compatibility/windows-7/partner/default.aspx). Even if a program isn't listed by Microsoft, there's a good chance it will still run on Windows 7.

If you encounter a program that won't install on Windows 7, try checking its compatibility properties. Right-click the setup program, select Properties from the context menu, and click the Compatibility tab. To change a program's compatibility level, select the *Run this program in compatibility mode for* check box, then select the desired OS from the drop-down list, as Figure 4 shows. For programs that simply won't install or run, you can use Windows 7's new virtualization-based compatibility capability, called Windows XP Mode (XPM).

Windows XP Mode for Windows 7

XPM for Windows 7 is essentially an updated version of Microsoft Virtual PC that includes a fully licensed copy of XP SP3. It's free for Windows 7 Professional, Enterprise, and Ultimate customers. Because XPM requires a virtualization-enabled CPU, your processor must have either Intel-VT or AMD-V support. You can use the SecurAble utility that I mentioned earlier to determine whether your CPU supports virtualization.

Unlike Virtual PC, in which every virtual machine (VM) runs in its own window, XPM uses a VMware Fusion–like capability to display a red-bordered window on the Windows 7 desktop that lists the names of applications running in XPM. When you install applications to the XPM environment, Start menu links and shortcuts are installed on the Windows 7 desktop as well.

XPM is a heavyweight, last-resort compatibility solution. It requires you to run a full VM, with a full copy of XP SP3, the Virtual PC software, and the XP application itself. Despite many overly enthusiastic claims, XPM doesn't provide 100 percent XP compatibility. The limitations of the Virtual PC environment prevent XPM from running many games or other applications that require advanced graphics capabilities. However, XPM does provide USB support, which is a nice improvement over Virtual PC 2007. To download the early release of XPM, go to www.microsoft.com/windows/virtual-pc/download.aspx.

Best OS Yet

Windows 7 is the best Windows desktop OS yet. Buying a new system with Windows 7 on it is the easiest way to upgrade from XP. If new hardware isn't in your future, you can still transition to Windows 7, with some effort. Although an in-place upgrade isn't possible, you can perform a clean Windows 7 installation and then use the Windows Easy Transfer utility to move your settings to the new installation. Windows 7's improved application compatibility and XPM let you run many programs that Vista couldn't. For more information about moving from XP to Windows 7, see the Microsoft article "Upgrading from Windows XP to Windows 7" (windows.microsoft.com/en-us/windows7/help/upgrading-from-windows-xp-to-windows-7).

InstantDoc ID 103144

Michael Otey
(motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

WINDOWS 7 UNDER THE HOOD

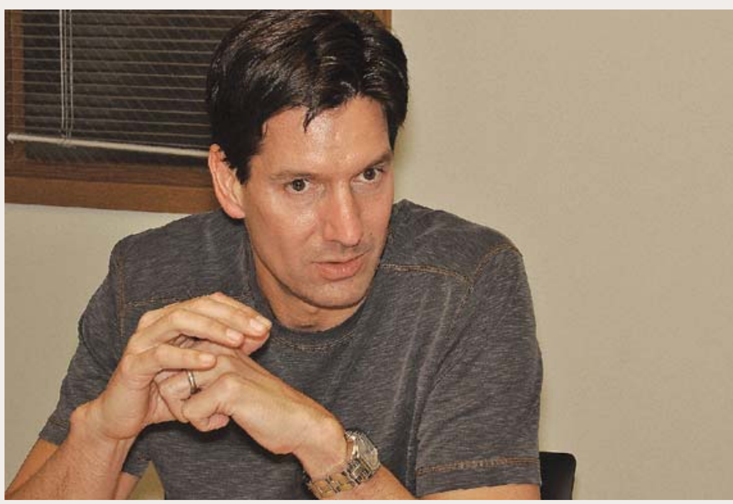
Microsoft technical fellow Mark Russinovich on what makes Windows 7 work—and what it owes to Vista

by Paul Thurrott

Photographs by Jim Molnar

Days after the official Windows 7 launch, *Windows IT Pro* analyst Paul Thurrott met with Microsoft Technical Fellow Mark Russinovich on the Microsoft campus to talk about the new client OS and its legacy. Russinovich was one of the earliest contributing editors to *Windows IT Pro* (*Windows NT Magazine* back in 1995), writing about Windows architecture from his perspective as a consultant and trainer who specialized in ripping into the Windows kernel. Russinovich first came onto Microsoft's radar with his notorious revelation in the November 1996 issue that Windows NT Workstation and Windows NT Server—which Microsoft sold with different licenses and portrayed as being capable of handling different workloads—had the same code base. The article's introduction set the stage: "Microsoft doesn't want you to read this article. At the kernel level, NT Server and NT Workstation are the same, and only a Registry key or two determines which is which. Just think about the implications." (You can find the original article at www.windowsitpro.com, InstantDoc ID 2816.)

In 1996, Russinovich started Winternals Software, which produced systems recovery and diagnostic tools, including Winternals Administrator's Pak, Protection Manager, Defrag Manager, and Recovery Manager. Microsoft acquired Winternals and Sysinternals (which offered free tools such as Filemon, Regmon and Process Explorer) in 2006, bringing Russinovich and business partner Bryce Cogswell on board. Russinovich now is on the Windows core architecture team, advising design teams as they bring the next versions of Windows to market. Following is his truly unique take on the forces that made Windows 7.



Paul Thurrott: So you're a technical fellow, but what is your actual job title?

Mark Russinovich: Well I call myself Chief Software Architect of Internals. I stole that from Bill. But my title is technical fellow.

Paul Thurrott: When you came to Microsoft, aside from bringing your tools, what was your involvement?

Mark Russinovich: I did some initial consulting with MS Dart and suggestions for features like the offline error scan. That's something we were planning on doing with internals.

Paul Thurrott: How do you look at Windows 7 from an architectural or foundational standpoint? [How did Microsoft] decide what was going to make Windows Vista into Windows 7?

Mark Russinovich: Windows Vista was very ambitious in a lot of different areas, it overreached in some areas, and there were features that were miscalculated. Example: What was that feature that you could walk up to someone's laptop with your laptop and share things?

Paul Thurrott: Right, Meeting Space. It was this feature that no one understood. There was no click: "Well, it's for peer-to-peer networking. You can go to a coffee shop." And I thought, "OK, I don't think anyone will ever use it."

Mark Russinovich: Windows 7 picked up where the Vista reset left off. We tried to be a lot more realistic about what could be done given the time frame that was set for the release. So with Vista, we were going after technology, going after features, and we'd figure out later when they all line up into a point where we can release a product. The Windows 7 release was: "OK, we've got three years, let's figure out what can fit in those three years and try to be as realistic and accurate as possible with our predictions." Things were mis-predicted, and things did get cut along the way. But it was on a much smaller scale. There was a big emphasis on the complete end-to-end scenario, so that this technology isn't just interesting from a technology perspective, but it's got to fit into something useful for the customer. So Vista did take a lot of the heat for things that now, in Windows 7, are accepted.

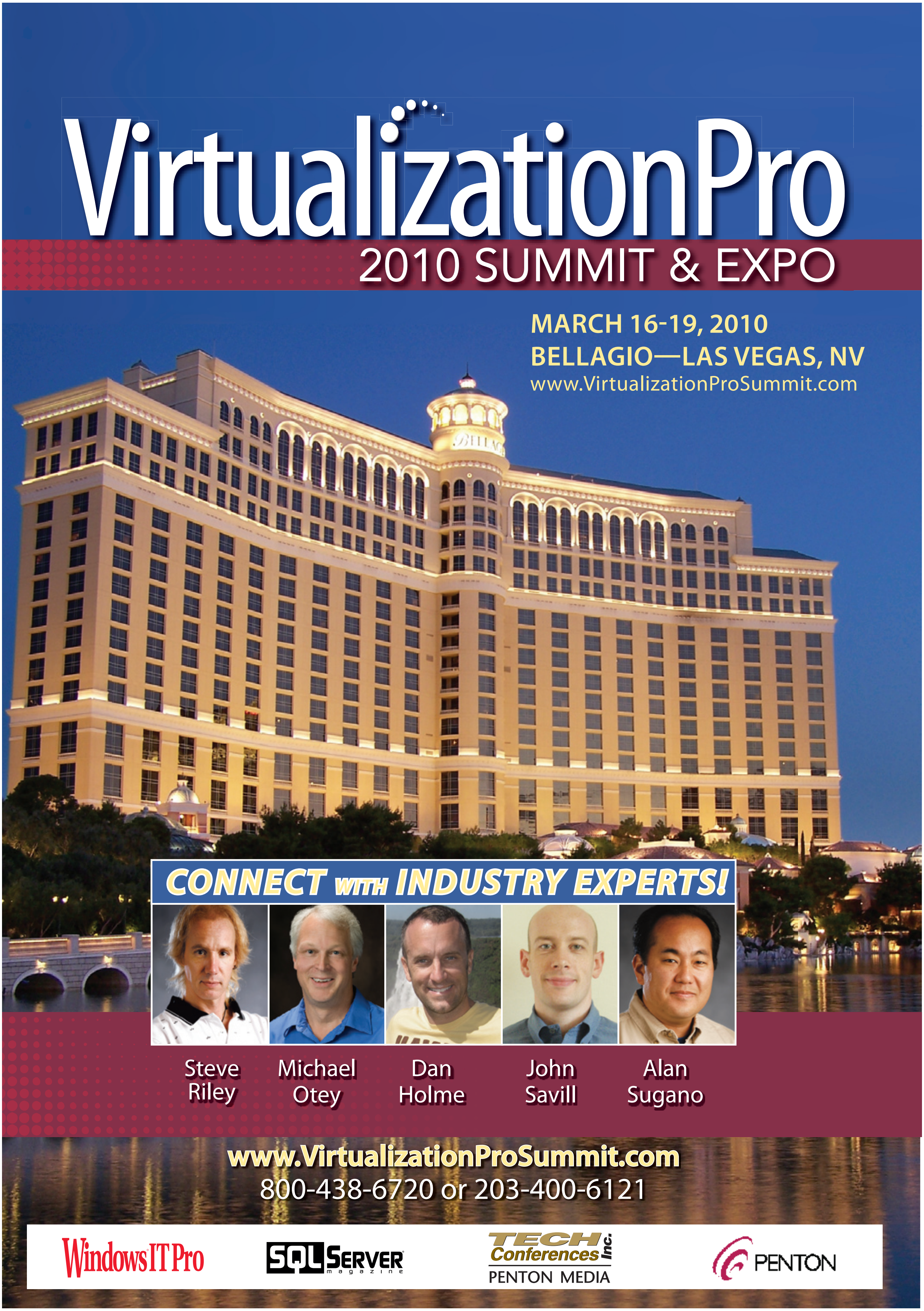
Paul Thurrott: I agree with you. There's a lot of history rewriting occurring here. Windows 7 could never have occurred without Vista, the way I look at it. So from an architectural standpoint, are there any major changes in Windows 7 compared to Vista on a deep level?

Mark Russinovich: As far as a system-churning kind of change, nothing really. As far as system-impacting things, there are a number of things. The biggest one at the lowest level of systems is Dispatcher Lock, the scheduling lock, that they got rid of. That has the biggest impact on things like server scalability. Power management—there was a big focus on that. Another thing you saw about this release versus the Vista release [was] a lot more collaboration with OEMs and hardware partners. So, for power management, there were really great interactions between us and Intel and AMD, [focused on] measuring power usage and optimizing the power profiles, working on things like Core Parking, taking advantage of the new processors, Deep [Power Down] C6 states.

And speaking of collaboration with the OEMs and hardware partners, another big effort with the Windows 7 release was going to the OEMs early and helping them clean up their systems. A lot of the bad rap Windows was getting, especially Vista, was because over time the OEMs were running out more and more stuff to try to get money off of a business that's got decreasing margins. So there's more and more of what's generally called crapware on these systems. Part of that was the OEMs didn't have the tools to know how the user was going to be impacted by these things or what to do about them. We shared a lot of our expertise. We had engineers work closely with their engineers, showed them how to use the Xperf tool in the Windows Performance Toolkit, showed them how to measure things. We even showed specific examples of where they had their own software bundled in the system that was starting out as the machine booted, and we'd give them recommendations on how to re-architect the software so that it was out of that path, since everyone measures boot time as something critical.

Paul Thurrott: That's true. I bet the big difference between a Vista PC and a Windows 7 PC in many ways—on the average PC—is in fact what you're describing here. The PCs, or the base install of the operating

Windows 7 picked up where the Vista reset left off. We tried to be a lot more realistic about what could be done given the time frame that was set for the release.


VirtualizationPro
2010 SUMMIT & EXPO
MARCH 16-19, 2010
BELLAGIO—LAS VEGAS, NV
www.VirtualizationProSummit.com
CONNECT WITH INDUSTRY EXPERTS!
Steve Riley
Michael Otey
Dan Holme
John Savill
Alan Sugano
www.VirtualizationProSummit.com
800-438-6720 or 203-400-6121
WindowsITPro
SQL SERVER magazine
TECH Conferences Inc.
PENTON MEDIA
PENTON

CONFERENCE INFORMATION

VirtualizationPro
2010 SUMMIT & EXPO

MARCH 16-19, 2010
BELLAGIO—LAS VEGAS, NV
www.VirtualizationProSummit.com

Top 10 Reasons to Attend the Virtualization Pro Summit

10 Learn how to take virtualization technology to the next level for the benefit of your organization.

9 Find out from industry insiders the best virtualization technologies.

8 Learn the differences between Microsoft Hyper-V and VMware ESX Server.

7 Choose from over 24 sessions delivered by industry experts.

6 Enroll to attend the VirtualizationPro Summit sessions and you can also attend any of the co-located Share-PointPro Summit sessions for FREE!

5 Attend sessions on current technology as well as highlights of the new stuff.

4 Extend your professional and social network at our events outside of the sessions.

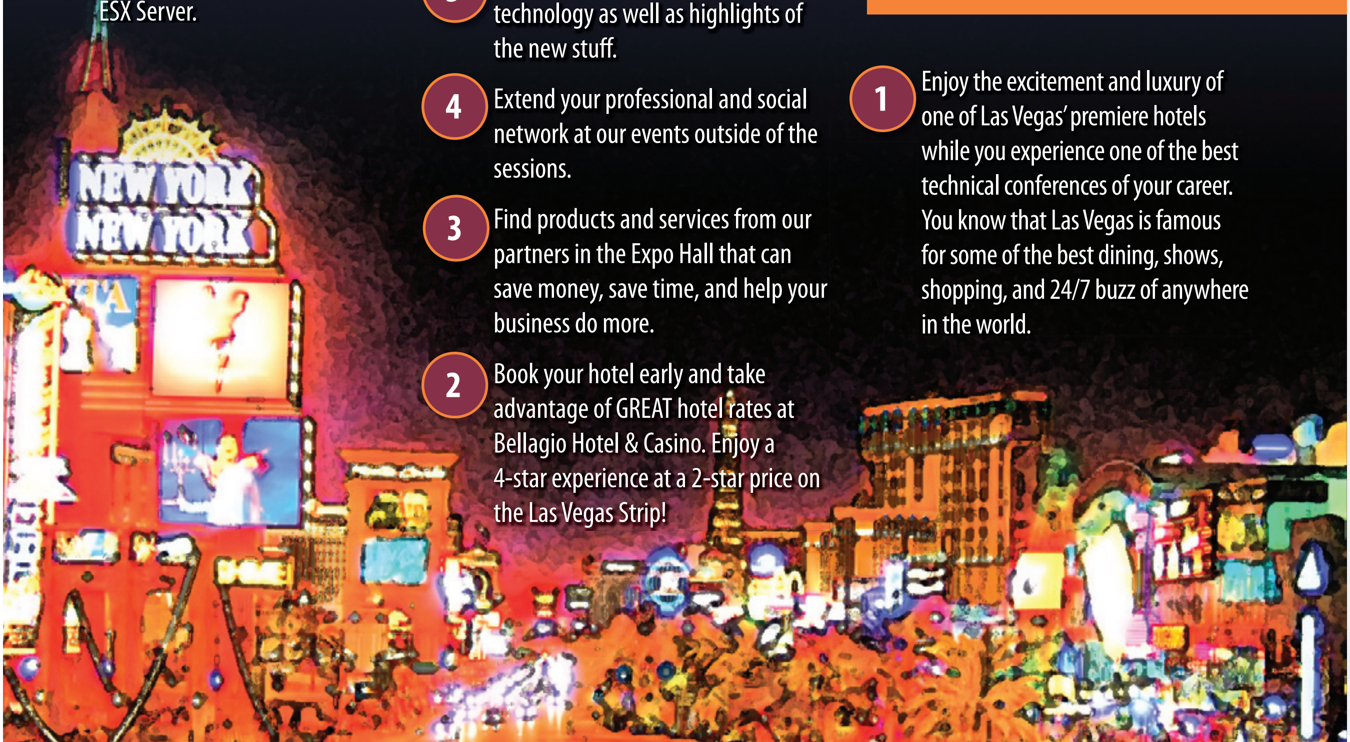
3 Find products and services from our partners in the Expo Hall that can save money, save time, and help your business do more.

2 Book your hotel early and take advantage of GREAT hotel rates at Bellagio Hotel & Casino. Enjoy a 4-star experience at a 2-star price on the Las Vegas Strip!

1 Enjoy the excitement and luxury of one of Las Vegas' premiere hotels while you experience one of the best technical conferences of your career. You know that Las Vegas is famous for some of the best dining, shows, shopping, and 24/7 buzz of anywhere in the world.

SCHEDULE at a glance

TUESDAY, MARCH 16, 2010	
7:30 am - 5:00 pm	Conference Registration
9:00 am - 4:00 pm	Pre-conference Workshops
6:30 pm - 8:30 pm	Opening Keynote
8:00 pm - 10:00 pm	Expo Hall Open
WEDNESDAY, MARCH 17, 2010	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 5:00 pm	Expo Hall Open
5:00 pm - 6:30 pm	Expo Hall Giveaways
THURSDAY, MARCH 18, 2010	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 4:00 pm	Expo Hall Open
FRIDAY, MARCH 19, 2010	
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions



Sean Deuby

Sean Deuby, a Senior Enterprise Solutions Strategist with Advaiya, Inc., has 25 years' experience in enterprise IT. He spent over a decade running Texas Instruments' IBM VM systems — the first virtualized operating system — then designed, deployed, and supported TI's first Windows NT 3.5 worldwide infrastructure. He also spent 10 years with Intel Corporation, where he was the design engineer of the core directory services team and one of the architects of Intel's corporate Active Directory forest. Sean has been a Contributing Editor for *Windows IT Pro* magazine for 10 years. Sean is a regular and highly rated speaker at Tech Ed and Windows Connections conferences.

Wendy Henry

Wendy Henry is a Microsoft Certified Trainer (MCT) who has been an independent technical trainer, author, and consultant for more than 10 years. She has specialized in Microsoft SQL Server since 1999 and SharePoint since 2005. Wendy is a contributing partner on SharePoint-eLearning.com and frequently teaches and presents at conferences on WSSv3/MOSS2007.

Dan Holme

A graduate of Yale University and Thunderbird, Dan has spent 15 years as a consultant and trainer, delivering solutions to tens of thousands of IT professionals from the most prestigious organizations and corporations around the world. Dan's company, Intelliem, offers deep expertise and experience in Windows, Active Directory, and SharePoint. From his base in beautiful Maui, Dan travels around the globe supporting customers and delivering Microsoft technologies training. Dan is also a contributing editor for *Windows IT Pro* magazine and a Microsoft MVP (Windows Server Directory Services, 2007, and Office SharePoint Server, 2008-2009). Dan is currently building SharePoint solutions to support the broadcast of the 2010 winter Olympics in Vancouver as the Microsoft Technologies Consultant for NBC Olympics.

Satish Jakka

Satish Jakka, Managing Editor at Platform Vision, has more than 15 years of experience. Before joining Platform Vision, he spent close to 10 years at Microsoft, where he worked as an Infrastructure Architect. Prior to that, Satish worked as a Senior Program Manager in the MSDN and TechNet product groups. Before Microsoft, Satish was Team Lead, Information Systems and Services for UUNET.

Heath Madison

Heath Madison, Director of Core Infrastructure at Advaiya, Inc., has been working in information technology since 1993 and specializes in Microsoft solutions. He has also served as a senior consultant and architect for implementing technology in global corporations. Heath has a thorough knowledge of Microsoft systems and solutions in addition to many third-party hardware and software tools.

Michael Noel

Michael Noel is an MVP for SharePoint Server and an MCSE+I. He has been involved in the computer industry for nearly two decades, and has significant real-world experience helping organizations realize business value from Information Technology. Michael has authored several major best-selling industry books that have been translated into seven languages with a total worldwide circulation of over 150,000 copies. Currently a partner at Convergent Computing in the San Francisco Bay Area, Michael's writings and worldwide public speaking experience leverage his real-world expertise designing, deploying, and administering IT infrastructure for his clients.

Michael Otey

Michael Otey, technical director for *Windows IT Pro* and *SQL Server Magazine*, is president of TECA, a software-development and consulting company in Portland, Oregon, and coauthor of SQL Server 2005 Developer's Guide (Osborne/McGraw-Hill). Michael has covered the topic of virtualization extensively for *Windows IT Pro* magazine, having written several features articles showing how to take advantage of virtualization in the enterprise as well as reviewing all of the major virtualization products.

Steve Riley

Steve Riley is an evangelist and strategist for cloud computing at Amazon Web Services, working to help organizations understand how to integrate their environments with the cloud to extend reach, increase utilization, and respond to rapid business changes. His specialties include information security, compliance, reliability, privacy, and policy. Steve is a popular speaker at conferences worldwide, meets regularly with user groups of all sizes, and seeks opportunities to engage with customers as often as possible.

John Savill

John Savill , Manager, Solutions Architecture at EMC, is a nine-time Microsoft MVP, and is recognized worldwide for his superior product knowledge and practical skills. He is the author of Windows Server 2003 Active Directory Design and Implementation, The Windows XP/2000 Answer Book, and The Windows NT and Windows 2000 Answer Book, and contributor to several Windows-related books in the "For Dummies" series of reference books. In addition, he serves as a contributing editor to various publications on Microsoft products including *Windows IT Pro* and *SQL Server Magazine*.

Alan Sugano

Alan Sugano is the president of ADS Consulting Group, Inc. (ADS), which specializes in networking, custom programming, Web development, SQL Server development, and ACCPAC Plus accounting implementations. Alan frequently delivers talks on network audits, server selection, network documentation, network management, network design and topologies, SQL Server databases, and disaster recovery.

PRE-CONFERENCE SESSIONS

Half-Day: (9am-noon) Virtual Desktop Infrastructure—Is It Really Something You Want or Need?

In this session we look at what VDI really entails, the architectural options we have for our design and the components needed. We will examine environments where VDI works well and how an organization goes about performing the business justification to really make sure VDI is something that they should be doing. Microsoft, VMware and Citrix technologies will be examined as possible solution points and how they can play well together.

Half-Day: (1pm-4pm) Implementing App-V

JOHN SAVILL

Virtualization is everywhere with Virtual Desktop Infrastructure gaining momentum in many environments. But one key technology is often overlooked and not fully understood: the virtualization of the applications. Formally known as SoftGrid, App-V is Microsoft's application virtualization solution. App-V allows the local execution of applications on an operating system without installing the application. The virtualization of applications solves two critical problems, application-to-application incompatibility and instant application launch for first-time use, which is crucial in any VDI scenario. In this session

we'll look at the underlying architecture of App-V, how exactly App-V functions and solves the mentioned application challenges, and best practices around App-V architecture and deployment through a live implementation of an App-V environment. At the end of the session attendees will have a strong understanding of how App-V works, when and when it shouldn't be used, and how to get App-V deployed in their environment.

Full Day: (9am-4pm) Technical Face-Off: Hyper-V and ESX

DEAN DEUBY, SATISH JAKKA, HEATH MADISON

If you're still trying to decide whether to implement Vmware's vSphere 4.0 or Microsoft's Windows Server 2008 R2 Hyper-V based virtualization solution, here's your chance to get the straight dope. Experts Sean Deuby, Satish Jakka, and Heath Madison of Platform Vision bring their Faceoff blog and poster (http://windowsitpro.com/faceoff) to life in this day-long session. Using examples and demonstrations, they will take an unbiased look at the two hypervisors and their management solutions, with the goal of helping you determine which issues are really important to you—and which are just hype. Topics will include the different hypervisor configurations, memory management, licensing, security, patch management, and the strengths and weaknesses of recommended management solutions from each vendor. This is a unique opportunity to learn from unbiased experts about the differences between each vendor's server virtualization solution so that you can make your own decisions based on side-by-side platform comparisons.

Keynote:
Stepping Into the Cloud

STEVE RILEY

Virtualization is one of the many key components of cloud computing. Indeed, without mature virtualization technologies and practices, cloud computing wouldn't be what it is today. And it's here to stay: unlike the application service provider days of the late 1990s, cloud computing is already changing the way many organizations store, process, and distribute information. Yet many other IT shops remain wary. Moving compute and storage out of your own data center and into someone else's, mingled among many others, seems daunting at first. Common questions arise around security, manageability, performance, and reliability. Think about it, though—these are the same concerns you've always had. Nothing about the cloud requires that you jettison everything you've learned during your career. The cloud is a logical next step in the evolution of computing, and when integrated with corporate IT removes much of the burden and allows a business to concentrate on its core functions. Steve Riley will introduce typical cloud architectures, explore common concerns, dispel several myths, discuss how to "think cloud," and help you learn how your business can benefit from the cloud.

BREAKOUT SESSIONS:

Virtualization and Security

STEVE RILEY

Securing an environment composed of virtual servers and clients presents certain distinct challenges, but it doesn't require you to throw away everything you already know. Virtualization follows a noticeable trend in the evolution of computing technologies; being aware of this helps us understand how to ensure that virtualized environments aren't suddenly vulnerable to attacks. Virtualization makes certain security-related tasks easier and more cost-effective, like application testing and deploying honeypots. Securing virtualized resources builds on the experience you already have and requires a few additional things to consider. Steve Riley will explore these topics and also examine security technologies deployed by Amazon Web Services in its implemention of the Xen hypervisor used in Amazon's Elastic Compute Cloud.

Highly Available Virtual Infrastructures

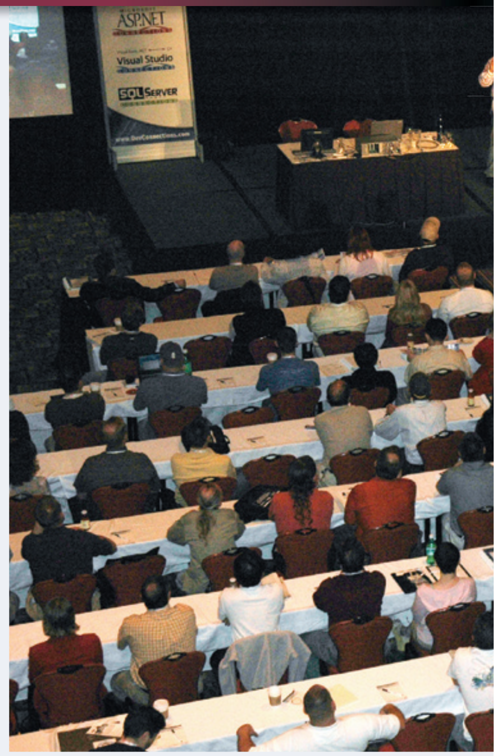
JOHN SAVILL

This session will explore technologies to help with planned and unplanned host downtime with both Hyper-V and VMware—and the pros and cons with the technologies used. We will also explore features related to storage and network migration without impacting guest instances.

Live Migration Step-by-Step

MICHAEL OTEY

In this session you'll learn about Hyper-V 2.0's Live Migration capability. You'll learn about requisites that need to be in place to



use Live Migration—and you'll follow along on a step-by-step guide to configuring and using Live Migration.

Virtualization of Exchange Server 2010 Architecture

MICHAEL NOEL

The advantages of server virtualization are significant and many organizations have been making the move toward virtualization of core components in their infrastructure, including Exchange Server. Virtualizing Exchange Server has certain significant challenges, however, and it is important to understand how to properly scale a virtualization environment to handle the unique requirements of Exchange. The latest version of Exchange Server provides for key virtualization advantages such as lowered Disk IO, multiple database copies using Database Access Groups (DAGs), and other enhancements that change the virtualization design paradigm. This session focuses on real-world best practice architectural guidance for virtualizing an Exchange Server environment, with particular focus on Exchange Server 2010 server roles and architecture. Real-world virtualized Exchange Server 2010 designs and deployments of varying sizes are discussed and compared.

- Understand how and when to virtualize Exchange Server 2010 server roles and components
- Determine the best virtualized Exchange Server architecture for your environment
- Learn the caveats, risks, and challenges that may be encountered in a virtualized Exchange environment

Server Virtualization Basics

ALAN SUGANO

As server hardware becomes more powerful, much of the processing power of the server is wasted. Server Virtualization allows you to efficiently use the processing power of new servers and the 64-bit platform by consolidating multiple physical servers onto a single virtual server host. We'll look at virtualization software technologies and how they work with server virtualization. We'll examine hardware configuration issues in the virtualization environment and offer tips on selecting the proper hardware for server consolidation. We'll review consolidation strategies to ensure that no one virtual server host is overloaded with virtual server guests. Virtualization has the potential to save money, reduce server setup time, provide a flexible test environment, speed up disaster recovery, and still provide high availability.

How Many Virtual Machines Can I Cram on This Box?

JOHN SAVILL

In this session, we'll examine the technologies that help achieve high virtual machine densities on your virtual infrastructure. We'll look at features that enable memory, CPU, and disk sharing between virtual machines and how Hyper-V and VMware can help consolidate on as few virtual servers as possible without impacting guest performance.

Designing Virtualized Storage for Resilience

Do you know where your VM data is? T-Mobile thought it did, right up to the point where all Sidekick users in the U.S. found their contacts and calendars missing. VM technology concentrates risk, which means you must design back-end SANs appropriately to mitigate those risks. Learn how to measure and counter vulnerabilities that arise out of having your eggs in an insufficient number of baskets.

ESX vs. Hyper-V

MICHAEL OTEY

Learn the differences between Hyper-V 2.0 to ESX Server 4.0 as Michael explores the architecture of the two products and compares their overall feature sets. You'll get an overall feature comparison as well as a cost comparison. You'll also learn about

the types of businesses each product is best suited for.

PowerShell Management for Virtualization: Hyper-V

SATISH JAKKA

Come learn how to use PowerShell to automate deployment and management of your virtualized infrastructure. See how you can leverage PowerShell across the Microsoft virtualization platform and go beyond to see PowerShell manage your applications through the entire application lifecycle.

Managing the User Experience across Physical and Virtual Environments

DAN HOLME

As enterprises turn to virtualization, in all its forms, users begin to "roam" in ways we never imagined just a few years ago. Even if a user sits at a single physical device, their experience stretches across remote desktop sessions, virtual machines, and virtualized applications. In order to maintain, let alone improve, productivity you must ensure a consistent, manageable and supportable workspace for your users. The pieces are all there: folder redirection, user profiles, group policy, ACLs, encryption, and DFS. But the intricacies and interactions of these technologies are surprisingly complex, and until you start managing them, your IT service delivery will suffer. In this session, you will learn best practices for putting the pieces together. Participants are expected to have a solid understanding of most or all of these technologies or be ready to learn them offline. This advanced session prepares you to take away ready-to-implement, useful solutions to corralling, securing, and managing user data and settings in both physical and virtual environments.

Virtualization's Role in Disaster Recovery

ALAN SUGANO

A comprehensive Disaster Recovery Plan is something that every company should have and hopefully will never have to use. Having a plan in place that provided a road map to recovery was adequate in the past, but recent emphasis has been placed on the speed of the recovery. Sarbanes-Oxley (SOX) compliance companies must disclose their business continuity plans and the company's exposure to a prolonged outage and how it affects financial reporting. Virtualization can significantly reduce the recovery time for a major disaster, by providing a warm or hot remote recovery site and accelerating workstation and server setup.

Understanding Virtualization Technologies

MICHAEL OTEY

Virtualization encompasses a virtual maze of technologies. Let Michael lead you through the maze as he explains the different types of virtualization. You'll learn about the difference in desktop and server virtualization as well as application virtualization. You'll also see where each of today's popular products fits in.

Virtualizing Your Active Directory Forest

SEAN DEUBY

Virtualization is all the rage today. Can you apply virtualization to the critical infrastructure of your Active Directory forest? When does

it make sense, and when should you leave it alone? Learn how to safely virtualize your domain controllers, understand security and recovery concerns, and apply virtualization to cheaply enable advanced domain recovery capabilities.

VMware: Performance Tuning and Configuration

SATISH JAKKA

Learn the art of tuning your VMware infrastructure for performance. In this session we will discuss the relationship between server workloads and CPU cores, memory, and storage. We will also discuss configuration, optimization and monitoring of workloads.

Automating the Dynamic Datacenter and Creating Virtual Machines Automatically

JOHN SAVILL

One of the key benefits of virtualizing the environment is a streamlined and accelerated provisioning process for operating system instances. In this session, we'll look at what a dynamic datacenter really is and the methods and technologies we can and should be using for the creation of virtual machines in our datacenter. We'll examine solutions from Microsoft and VMware. And in addition to just creating our virtual environment, we'll see how to maintain the datacenter most efficiently and how to automate provisioning of virtual environments for end users.

Has Virtualization Decreased the Importance of SQL Server Backups?

WENDY HENRY

So, how long does your hardware take to perform a full backup and restore of your largest SQL Server database? As virtualization platforms have matured, so have the underlying storage facilities smart networks employ to reap the hardware utilization and ROI benefits of virtual machines without suffering performance degradation. Many virtualization and storage platforms offer advanced snapshot and availability features that you can use to redirect users to previous versions of mission-critical data without the delays of traditional restore operations. Have these features eliminated the need for traditional backup and restore disaster recovery strategies? In this session, we'll explore the idea of using virtual versioning and archiving in place of traditional SQL Server database backups to satisfy the immediate access demands of today's business users.

A Compelling Look at vSphere 4.0

ALAN SUGANO

vSphere 4.0 is VMware's next release of their Hypervisor. It represents VMware's move from a 32-bit Hypervisor in ESX 3.5 to a 64-bit Hypervisor in vSphere 4.0. The performance improvement, especially in CPU-intensive applications, is significant. In fact, you could justify the upgrade based on the improved performance alone. Besides the performance aspects there are a significant number of new features in vSphere, Some including

1. vSphere Bundles
2. 64-bit Hypervisor
3. Host Profiles
4. VMKernel Protection
5. Improvements in Fault Tolerance
6. VMotion Enhancements
7. vShield Zones
8. Hot Add Support
9. Power Management
10. Thin Provisioning
11. Fibre Channel over Ethernet (FCoE) Support
12. vNetwork Distributed Switch

Learn about these new features and how they can benefit your company's virtualization IT strategy.

Distributed File System: The Cheapskate's Storage Virtualization

SEAN DEUBY

Microsoft's Distributed File System provides a way to easily separate how your users access their data from where the data's located on your network. And it needn't cost you anything to implement it! Learn how to use it to quickly and easily build, manage, and delegate an easy to use enterprise virtual folder structure.

PowerShell Management for Virtualization: VMware

SATISH JAKKA

Come learn how to use PowerShell to automate deployment and management of

your virtualized infrastructure. See how you can leverage PowerShell across the VMware virtualization platform and go beyond to see PowerShell manage your applications through the entire application lifecycle.

vSphere vs. System Center

MICHAEL OTEY

Come to this session to learn how vSphere compares with Microsoft's System Center. You'll get an overall feature comparison as well as see how each product addresses different management concerns in the organization.

Application Virtualization

ALAN SUGANO

End the patch management hell. Application virtualization allows you to run applications without having to install the application on each workstation. This simplifies patch management and significantly reduces the time to roll out new or upgraded applications, because patches are installed once on the application server and not individually on each workstation. We'll take a look at Microsoft's Softricity technology and how it handles local, remote, and disconnected clients and their applications. This technology also leads to the software as a service directive that many companies see as an industry trend. Application virtualization also ties into disaster recovery because it significantly reduces the prep time for workstation recovery. Application virtualization can reduce patch management headaches, reduce the time to roll out new applications, easily roll back problematic patches, allow users to run different versions of the same application, and speed up disaster recovery. See if this technology is a good fit for your company.

System Center Virtual Machine Manager: Real Control for Your Virtual Environment

SEAN DEUBY

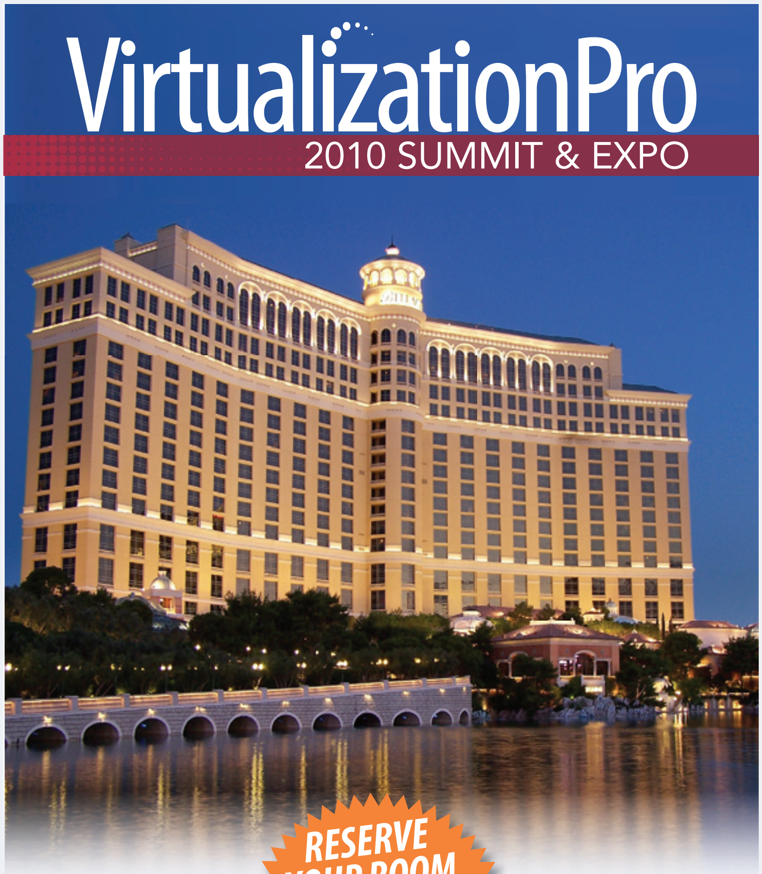
Managing your Microsoft or VMware virtual machines presents a different set of challenges than managing physical servers. Virtual systems move around on different physical hosts, they can be quickly provisioned or de-provisioned, their large disk images present unique management, security, and performance challenges…the list goes on. Microsoft's System Center Virtual Machine Manager (SCVMM) is designed to handle all these challenges of managing virtual systems from both Microsoft and VMware, from workgroup-sized configurations to full enterprise deployments. Check out this session to learn how to quickly begin using SCVMM to manage your virtual environment.

Virtualization of SharePoint 2010 Farm Architecture

MICHAEL NOEL

Server virtualization technologies have taken center stage recently and many organizations have begun to replace physical servers, including SharePoint servers, with virtualized machines. Virtualization of the 2007 wave of SharePoint Products and Technologies has been supported for some time, and many 2007 farms have been successfully virtualized over the years. With a new version of SharePoint, however, comes new best practices and new techniques for virtualization of SharePoint. This session focuses specifically on SharePoint Server 2010 farm virtualization and how components of a SharePoint 2010 environment can be successfully virtualized. Included in the discussion are new virtualization high availability options such as Windows Server 2008 R2 Hyper-V Live Migration of SharePoint guest sessions as well as time-tested design architecture examples using integrated SharePoint failover techniques.

- Learn the best practices for virtualizing the new architectural elements of a SharePoint 2010 farm
- Examine real world designs of virtualized SharePoint farms of varying sizes and functions
- Understand how to properly size a SharePoint environment by reviewing real world sizing guidelines for virtual hosts, guests, server and storage infrastructure



RESERVE YOUR ROOM EARLY to take advantage of great hotel discounts!

HOTEL ACCOMMODATIONS

Bellagio Las Vegas
3600 Las Vegas Blvd South
Las Vegas, NV 89109

Bellagio Las Vegas is the conference site and host hotel. This is where all sessions and activities are held. Hotel requires a one night's deposit at time of reservation. (Credit card will be charged by the hotel). Hotel cancellation policy: Must cancel at least 72 hours prior to arrival date.

The special conference rate will be honored starting two days before the start of conference through two days after the end of the conference, based upon availability. Space is limited so reserve your room early by registering online or by calling the conference hotline at 800-438-6720 or 203-400-6121. All reservations must be guaranteed with a major credit card to confirm room. A deposit of the first night room and tax will be charged. Cancellations must be received by the hotel 72 hours prior to the confirmed arrival date to receive refund of deposit.

TRANSPORTATION

Taxis are available right outside of the baggage claim area of McCarran International Airport. Taxi Ride will average approximately $18.00 (subject to change) to the Bellagio Las Vegas.

ATTIRE

Conference dress is comfortable and casual. Temperatures in Las Vegas are about 68º F (20ºC) in March. The session rooms are air conditioned so you may want to bring a sweater.

TAX DEDUCTION

Your attendance to the VirtualizationPro 2010 Summit & Expo may betax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

1-3 registrants: $1,395 per person

Additional registrants after the 3rd: $1,195 per person ($200 off each)

Call 800-438-6720 to take advantage of group discount pricing.

NOTES & POLICIES

The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.VirtualizationPro-Summit.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague by notifying us before the start of the event. Please inform us if you have any special needs or dietary restrictions when you register. The conference registration includes the following subscription. This is not an additional expense and subtraction from prices listed is not permissible. VirtualizationPro 2010 Summit & Expo registration includes a one year (12 issues) print subscription to Windows IT Pro magazine. Current subscribers will have an additional 12-months added to their subscription. Subscriptions outside of the United States and Canada will be served in digital; $12.50 of the funds will be allocated toward a subscription to Windows IT Pro magazine ($49.95 value).

Registration & Cancellation Policy: Payment must be received before the start of the conference. Cancellations by February 15th, 2010 must be received in writing and will be refunded minus a $100 processing fee. After February 15th, 2010 cancellations and no-shows are liable for full registration fee, however registration can be transferred to the next Conference within 12 months or to another person.

CONFERENCE REGISTRATION

ONLINE
www.virtualizationprosummit.com

PHONE
800.438.6720
203.400.6121

FAX
913.514.9362

MAIL
VirtualizationPro Summit & Expo
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Name | Priority code

Company | Title

Street Address (Required to ship materials)

City, State, Postal Code | Country

Telephone | Fax | E-mail Address (important)

VIRTUALIZATIONPRO 2010 SUMMIT & EXPO	PRICE	SUBTOTAL
on or before January 15, 2010	$1195.00	
after January 15, 2010	$1395.00	
Early Bird Bonus: Register for the conference and hotel (on or before January 15th) and receive a $100 Bellagio Gift Card. (3 night minimum stay at host hotel required)		

PRE-CONFERENCE WORKSHOPS | Tuesday, March 16,2010 | Lunch is included with full day workshops			
Half-Day (9 AM - 12 PM)	Virtual Desktop Infrastructure --Is It Really Something You Want or Need?	$199.00	
Half-Day (1 PM - 4 PM)	Implementing App-V—John Savill	$199.00	
Full Day (9 AM - 4 PM)	Deep Dive Comparison of Hyper-V and ESX—Sean Deuby and Satish Jakka	$399.00	

PAYMENT

TOTAL

*IMPORTANT: You must reference VirtualizationPro Summit & Expo on your check.

☐ CHECK (payable to Tech Conferences) All payments must be in US currency. Checks must be drawn on a US bank.

☐ VISA ☐ MASTERCARD ☐ AMEX

Cardholder's Signature

Cardholder's Name (rint)

VirtualizationPro
Summit & Expo
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 0648

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

system, might boot in whatever percentage. But once you start adding all that stuff, if the PC makers are working with Microsoft more, those things probably start up a lot more quickly simply because of the way they're designed.

Mark Russinovich: Yes, our performance team looked at systems across the board, sample systems from a whole bunch of OEMs running all sorts of performance tests on them. We did this with the antivirus companies as well.

Paul Thurrott: So give me your thoughts on this: One of the early debates for Windows 7 was whether it is a minor or major release, which is a semantic issue in many ways. But I look at it from a technology standpoint, from the perspective of people who have to manage and support the systems. It's sort of a minor release because it's the same technology, essentially—a very familiar environment. But from the end-user perspective, it's a major release, because there's lots of good stuff going on in the UI. Was that even a consideration? How does Microsoft view this?

Mark Russinovich: Steven Sinofsky and John DeVaughn didn't view this release as minor or major. It's a release. This is the cadence that we want to ship Windows by, so this is the kind of stuff we could get into the release, given this cadence. We expect that the changes they've made organizationally will make the system more efficient, and make it possible to get more work done in a shorter period of time. So there might be more work done in a Windows 8 time frame than a Windows 7 time frame.

Paul Thurrott: Obviously there's a new plan in place, and I'm sure it's a new team in many ways. So given the success of this system, it seems like this is the way it's going to go for a while. So the plan is that Windows 8 might occur in a similar time frame. But you're saying that because of the efficiencies, it's possible that there might be even more of a change?

Mark Russinovich: Yes.

Paul Thurrott: From an upgrade/migration picture, one of the easy complaints for Windows 7 is it doesn't provide for in-place upgrades from XP. What went into that decision and what are the real issues there?

> We expect that the changes [Microsoft has] made organizationally will make the system more efficient, and make it possible to get more work done in a shorter period of time.

Mark Russinovich: Well, when you do an in-place upgrade, the test matrix for that is enormous. So, obviously, if we're going to do an in-place upgrade, the most recent operating system is a higher priority than an older operating system that people are going to be coming from. From an enterprise perspective, it's really not an issue because people don't upgrade their systems, they do clean installs. From a consumer perspective, if you look at people running XP systems, they're probably running older hardware that's not even in the class of Vista/Windows 7 where it would make sense to do an upgrade.

In addition, if you look at trends in the past, consumers don't upgrade either—they buy new PCs and get the new version of the operating system. So if you look at the return on investment of supporting the XP to Windows 7 upgrade path, versus the people that would actually benefit from making it easier than it is with the migration tool, it didn't seem to make sense.

Paul Thurrott: So then from a general perspective of IT pros, what are the big benefits you see for Windows 7? What are their reasons to migrate to Windows 7?

Mark Russinovich: There are a few big benefits that will come when you pull in [Windows] Server 2008 R2. So there's a big benefit, but it's also a fairly good-sized investment to get to that benefit—things like BranchCache and Direct Access. If you look at just the Windows 7 client itself, you get a more efficient system, and the fact that end users can do things more efficiently—they're happier with UI changes. So there are a whole bunch of little things—the troubleshooting packs, which you can custom write, and a bunch of them built in. The Resource Monitor is vastly improved over what was in Windows Vista—in fact, it seems like a lot of the Sysinternals-type functionality up to a certain point.

Paul Thurrott: Looking within the context of the good/better/best kind of stuff, obviously Microsoft has the server things going on with R2 and then the MDOP [Microsoft Desktop Optimization Pack] stuff. If you could only do one, which makes the most sense?

Mark Russinovich: Server, MDOP, or client?

Paul Thurrott: Yes.

Mark Russinovich: Well the MDOP people would say MDOP. I guess I didn't even address the Server 2008 component. Virtualization delivers massive improvements there, Live Migration being the big key feature. But lots of scalability and performance improvements, and Hyper-V R2. That's obviously a really important workload these days. The AD Recycle Bin. It's the little things.

Paul Thurrott: Yes, it is the little things. That's almost the message for Windows 7 when you think about it.

Mark Russinovich: I think if you got a lot of little things that are nice, and don't have any big things detracting from it—driver incompatibilities and application incompatibilities—then all those little things add up to something decent. But when you have a problem like Vista had coming out the door, it can wipe out even bigger things in terms of the value people see.

Paul Thurrott: What about security?

Mark Russinovich: BitLocker To Go is a big thing. And that's again built on the foundation of stuff that was introduced in Vista. AppLocker—I'm personally passionate about that whole whitelisting space because the last product Winternals made was a product called Protection Manager, which was a whitelisting product. So AppLocker is a better inbox whitelisting solution than SRP [Software Restriction Policies] was previously. AppLocker has some of the things that Protection Manager and some of the third-party products set up before, like being able to authorize software based on a certificate and other metadata, especially with the image like the publisher and version number.

Paul Thurrott: It's interesting in the next version of MED-V that they're going with the previous version of Virtual PC for compatibility purposes. It doesn't require [particular CPU support, like Windows Virtual PC and XP Mode]. Do you see virtualization having a bigger impact on the client side going forward?

Mark Russinovich: First of all, App-V really brings you two things. One is the streaming, so being able to run software without having to pull it down and install it. And then secondly is the isolation—the isolation is something that they do underneath the application because the application model that Windows evolved with doesn't cleanly separate application data between system settings, user data, and user settings. So that's what App-V is doing under the hood—dynamically figuring out where those pieces of data are and separating them. That's what the whole sequencing does is figure out where those things are.

If we could get everybody to rewrite their apps and separate them, and then put streaming on top of that, you'd basically have App-V, or what you wanted from App-V: Being able to have applications side by side, and having the dependencies nicely identified, their states separated so you could toss changes and go back to a good point. So the way I see App-V evolving is us trying to go in that direction with applications in general, not just relying on this trick underneath.

And as far as virtualization on the client, this is something that we've thought long and hard about, and are still thinking long and hard about, and the question is: Are there any scenarios where there's compelling value to having machine virtualization on the client that makes up for the increased management cost and performance degradation that you would get out of it? If you take any particular scenario where you say, "We could do that with machine virtualization," then what we do is say, "Well, is there any way you could do that with VPC type of virtualization, or within the Windows box, and does that make more sense?" So, what is the value that the machine virtualization is bringing?

Paul Thurrott: I think any form of virtualization, regardless of where you go, gives you an interesting way to cut with the past, because by providing a previous version of Windows in a VM, all of a sudden there are these old APIs that you don't have to include now in the base system.

Mark Russinovich: We'd love to be able to move on to a newer, better, more coherent world, but mixing the old and new is something people are going to want to do. From a UX perspective and from an application interoperability perspective, from a systems management perspective—that's where all the seams in machine virtualization show up and cause problems. You can patch over some of it, with things like the integration stuff in XP Mode where things show up in the Start menu, but it's still not seamless from a management perspective or a UX perspective.

Paul Thurrott: Apple recently described Windows 7 as old technology, which I found somewhat hypocritical given that UNIX is the basis of Mac OS X. How do you react to a comment like that? I mean, obviously there's old stuff.

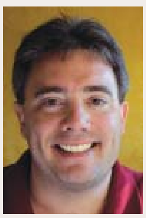
Mark Russinovich: The value of Windows is that it's old technology that runs everyone's apps. If we came out with an OS that looked like Windows but couldn't run your Windows apps, it wouldn't be Windows. Nobody would want it.

Paul Thurrott: It'd be Ubuntu.

Mark Russinovich: Yes, it'd be Ubuntu. It'd be something else. And so, the value of Windows is being able to carry things forward and improve the experience—manageability, security, reliability—along the way.

InstantDoc ID 103218

If we came out with an operating system that looked like Windows but couldn't run your Windows apps, it wouldn't be Windows. Nobody would want it.



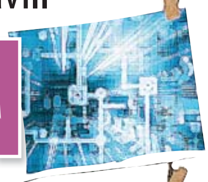
Paul Thurrott

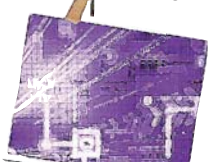
(thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

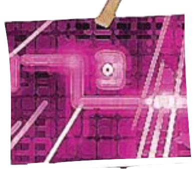
USING ACTIVE DIRECTORY SNAPSHOTS AND THE DSAMAIN TOOL

AD backups made easier

by John Savill







Active Directory (AD) is one of the most important containers of information in the entire Windows environment. Not only does it store all the users, groups, and computers but it frequently acts as a container for configuration information for other services throughout the organization. An AD failure or loss of data would mean a huge outage for any environment.

Fortunately we have multiple safeguards in place for AD. First, it's a multi-master directory, which means multiple servers host their own copy of the AD database, ntds.dit, so if one domain controller (DC) fails there are always other DCs to provide directory services to the organization. No DC is considered special—you can remove or lose any DC and stand up another in its place at any time, which is the beauty of the multi-master replication model. Second, backups of AD can capture the entire content of AD, which can be restored from a historical point in time.

This actually brings us to an important point: Because of the multi-master nature of AD, it's rare to restore a backup in the event we lose a DC. You just create a new DC and replicate the database from another DC.

However, what happens when you accidentally delete an object or a whole organizational unit (OU) of objects? (The most common cause of deletions is, after all, user error.) The deletion is replicated to all the other DCs, so you can't just copy the deleted object back from another DC.

With Windows Server 2008 R2 you can enable the Recycle Bin, so deleted objects can easily be restored. But prior to Server 2008 R2, or if this feature isn't enabled, you need to bring the object back from a backup or use third-party tools to try and reanimate the deleted objects. However, this reanimation loses most of an object's attributes and all group memberships.

Even if you use the Recycle Bin in Server 2008 R2, you might need to restore an object to a previous version, so backups might still be required. The Recycle Bin doesn't store historical copies of an object, and only an object that's deleted makes it to the Recycle Bin.

AD backups aren't pleasant to work with. You have to boot a DC into a special Directory Services Restore Mode (DSRM), which means the DC no longer offers directory services. Then you must restore a backup of AD and manually mark the objects you want to restore as authoritative, so they don't get overwritten or deleted as soon as the DC is rebooted and starts replicating again.

Imagine not knowing which backup has the right version of an object you want, or being in an audit situation and needing to know what changed on an object. Manually restoring every backup to a DC through DSRM would be very time consuming. Even when you find the right backup, it's very hard to do comparisons between the content of the backup and the live AD.

Active Directory Database Mounting Tool

Server 2008 introduced a solution to check the content of an AD backup without going through a painful restoration process. The Active Directory Database Mounting Tool, Dsamain.exe, allows an ntds.dit file to be mounted and exposed as an LDAP server, which means you can use such familiar tools as ADSIEdit, LDP.exe, and Active Directory Users and Computers to interact with a mounted database. Obviously because you're mounting on a DC, you can't mount the AD database as the standard LDAP port of 389 but a custom port specified during the mount operation. Once it's mounted, you can access both live AD content and AD content as it existed when the ntds.dit backup was taken.

I'll show this in action later in the article. First, though, there's one other important technology that goes along with the AD database mounting tool that, while not required, is extremely useful.

Active Directory Snapshots

To obtain a backup of AD you use backup software that calls the NTDS Volume Shadow Copy Service (VSS) writer, which is part of the VSS solution for each application or service and ensures the AD information on the disk is in a consistent state so it's suitable to be backed up. You can view the NTDS VSS writer through the vssadmin list writers command.

After you get a backup taken through VSS, you can open up the backup and extract the ntds.dit file, copy it somewhere, then mount it with the Dsamain tool, as we'll see shortly. If you're using the Server 2008 backup utility to perform system-state backups, you could mount the virtual hard disk (VHD) file created natively by the in-box backup application in Server 2008 R2. You could mount it through the Disk Management snap-in or through the VHDMount tool with Server 2008 and just copy the ntds .dit file to a temporary location.

You could use another method, however, which works with normal backups and might be preferable for some environments. Using the same NTDS VSS writer, you can actually create snapshots of AD in-place on the DC, letting you keep point-in-time copies of AD locally for easy access.

We have seen this technology before with shadow copies of file shares that let you see file shares as they existed at previous points in the past. This is exactly the same; we take snapshots of AD at certain points in time and interact with them via the Dsamain tool.

So how much space do these snapshots actually use up? If you're at a large company with a multi-gigabyte ntds.dit file, you need to factor in the disk space usage of these snapshots. Actually, the only disk space used is for the differences between AD and the point in time the snapshot was taken.

A copy-on-write approach is taken, which means when you first take the snapshot there's no difference between the snapshot and the live AD, so the size of the snapshot storage is basically zero. As AD changes, the old data in AD that's being replaced by the new data is copied to the snapshot storage so the snapshot contains only the delta (difference) data. The more changes you make to AD, and the longer the snapshot remains, the larger the snapshot will become as the delta increases.

When you want to use a snapshot, it basically combines the information in the snapshot with the information in AD that hasn't changed since the snapshot was taken. Obviously there's a slight performance impact using a snapshot, as now any write to AD will first require the data being replaced to be copied to the snapshot storage. The good news is that snapshots chain together, so if a daily snapshot is taken, then each snapshot contains only the delta information from the day the snapshot was taken until the time the next snapshot is created.

At this point you might wonder if you even need to bother with a backup at all. Looking at the development of Server 2008, initially the in-box backup application wasn't going to support system-state backup, so the directory services needed its own mechanism, which became AD snapshots. However, the backup team then decided to add system-state support, so the mechanisms to actually restore from a snapshot were never implemented.

This means you can't perform a restore from a snapshot, and to actually perform object recovery in a supported fashion, you still need backups. However, thanks to AD snapshots, you likely won't need to use the backups as often.

Note that an AD snapshot and a system-state backup don't contain the same information. While an AD snapshot basically contains information related to AD, a system-state backup also contains the information needed to restore the entire OS. Thus, an AD snapshot is considerably smaller than a system-state backup.

Using AD Snapshots

Now let's actually manage some snapshots and use them. Remember, you don't have to use an AD snapshot—you can use the ntds .dit file extracted from a backup. However, for this example I focus on AD snapshots (which are just containers for ntds.dit copies).

You use the NTDSUTIL utility to manage snapshots. The steps to manage snapshots involve activating the NTDS instance, then issuing the create command:

```
C:\Windows\system32\ntdsutil.exe: snapshot
snapshot: activate instance ntds
```

returns *Active instance set to "ntds"*

```
snapshot: create
```

returns *Creating snapshot...Snapshot set {02eb0c44-701c-4a82-97d1-e3f938844867} generated successfully.*

You can combine all of these commands into a single line for easy execution or for scheduling snapshot creation:

```
ntdsutil "activate instance ntds"
  snapshot create quit quit
```

To create a list of the snapshots, use the following command:

```
snapshot: list all
```

which returns this list:
1: 2009/10/04:12:19 {02eb0c44-701c-4a82-97d1-e3f938844867}
2: C: {5c69a713-98a5-4a97-8aed-c6ce528e8de4}

Notice that although I took a single snapshot, I actually have two entries. When you take a snapshot, you get a snapshot entry for the complete snapshot that encompasses all the volumes in the snapshot. You then have an entry for each volume.

In this case, only one volume is in the snapshot because the system drive, AD database, and AD logs are all on the C drive. However, if the AD database and AD logs were on different drives, you would also see entries for the volumes containing the database and log files.

To delete a snapshot you have a choice of two commands. Simply type

```
delete <snapshot number>
```

or

```
delete <snapshot GUID>
```

Now that we have a snapshot, we need to mount it onto the file system so we can then access the ntds.dit file contained within the snapshot. Until the snapshot has been mounted it's not visible in Explorer.

Once mounted, a new folder will be created on the system drive in the format of $SNAP_<date time of snapshot>_VOLUME<volume>. For example, I created $SNAP_200910041219_VOLUMEC$.

To mount it, we use the mount command with either the snap ID or the snap GUID:

```
snapshot: mount {02eb0c44-701c-4a82-
  97d1-e3f938844867}
```

and we are told the folder where the snapshot has been mounted:
Snapshot {5c69a713-98a5-4a97-8aed-c6ce528e8de4} mounted as

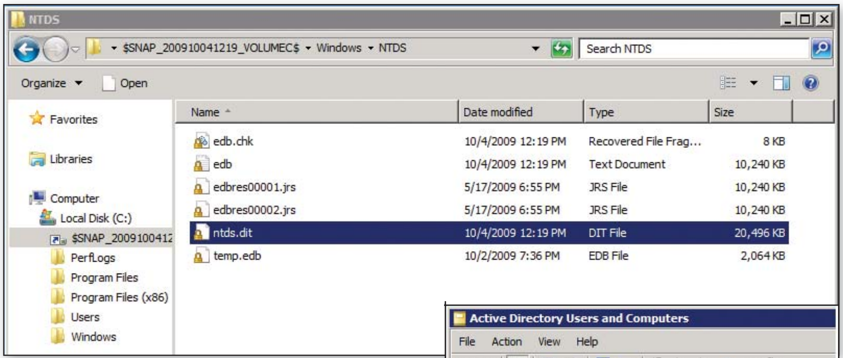


Figure 1: Mounted snapshot

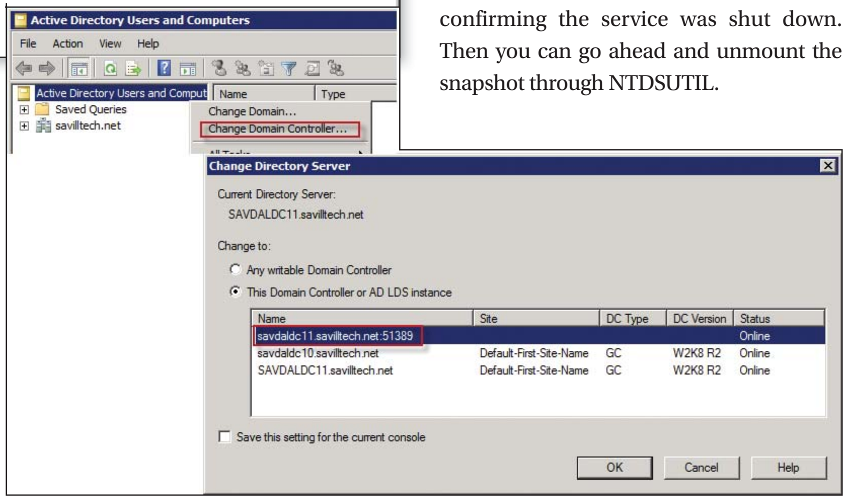


Figure 2: Accessing a snapshot through Active Directory Users and Computers

C:\$SNAP_200910041219_VOLUMEC$\.

Once a snapshot is mounted it will stay mounted until manually dismounted. Also note that I mounted the main snapshot ID, which then mounted the volume snapshots that it contained. We can now open Explorer, see that the snapshot is available, and browse its content, including the C:\Windows\NTDS folder, which Figure 1 shows.

Security is maintained: The permissions you have on the files in the snapshot are the same permissions you had when the snapshot was taken. To dismount, use the unmount command, passing the GUID or snapshot ID:

```
snapshot: unmount {02eb0c44-701c-4a82-
  97d1-e3f938844867}
```

Now you can use the Dsamain tool to offer LDAP services to the ntds.dit file you've exposed through a snapshot or that you copied from a backup. Open an elevated command prompt window and pass the dsamain command path to the ntds.dit file through the /dbpath switch and the LDAP access port through the /ldapport switch:

```
C:\>dsamain /dbpath
  C:\$SNAP_200910041219_VOLUMEC$
 \Windows\NTDS\ntds.dit /ldapport 51389
```

You must include ntds.dit in the path, and remember also that you can't use port 389 for the LDAP, as the live AD will be using this; it's common to use port 51389 instead.

An event log is generated notifying you that the database is mounted. Keep the command-prompt window open as it contains the dsamain process that's hosting the access.

Although we only passed an LDAP port number, the Dsamain process also opened ports for LDAP-SSL, Global Catalog (GC), and Global Catalog-SSL. The port numbers assigned are just increments of the port we passed for LDAP, so if we passed 51389 for LDAP, then port 51390 would be used for LDAP-SSL, 51391 for GC, and so on. If you want to use specific values, then use the /sslPort, /gcport, and /gcsslport parameters.

If you have an ntds.dit file from an earlier version of Windows, you can open it via the /allowupgrade switch. Another useful switch is /allowNonAdminAccess, which as the name suggests, allows non-domain and non-enterprise admins to access the data.

We can now access data by using the standard tools and scripts. The only difference is we can't use the default ports for LDAP, GC, and the others; we need to pass the ports we have specified.

Let's use Active Directory Users and Computers: Start it as normal (DSA.msc), then right-click the root of the navigation and select Change Domain Controller. Choose *This Domain Controller or AD LDS instance* and type in the IP address and port as shown in Figure 2. You are now accessing the snapshot copy of AD.

Numerous tools are available that compare AD instances and use data in the snapshot for purposes such as object reanimation. A good one is the Directory Service Comparison Tool, which can be found at lindstrom.nullsession.com/?page_id=11. After you perform the analysis, close the Dsamain instance offering the access by pressing Ctrl+C, which writes a 1004 event confirming the service was shut down. Then you can go ahead and unmount the snapshot through NTDSUTIL.

A Good Start for a Great Feature

As you can see, just because you can't directly restore objects from a snapshot or backup exposed via Dsamain doesn't mean it's useless. You can use tools to do comparisons between a snapshot and another snapshot or the live AD, and you can copy attributes from a snapshot in the live AD—you just can't perform a traditional restore and keep attributes such as SID. You can use the information exposed through Dsamain to make sure you have the right backup from which to restore or use it to get the information you need to perform an object reanimation. The AD snapshot feature is a great tool for AD admins; I can only hope in the future its role expands to actually allow object restoration.

InstantDoc ID 103091

John Savill (john@savilltech.com) is an advisory architect for EMC's Microsoft consulting practice. He's an MCITP: Enterprise Administrator for Windows Server 2008, CISSP, VMware Certified Professional and a ten-time MVP. His latest book is *The Complete Guide to Windows Server 2008* (Addison-Wesley).


We would never tell a lie...
... but we've been caught bragging now and then.
That's why we're going to let our readers tell you why *Windows IT Pro* is the top independent publication and Web site in the IT industry.
So, direct from our readers' mouths (yes—really)!
"The best windows environment magazine around—BAR NONE!!" —Joe A. Chief, Technical Section
"No other magazine consistently provides timely, relative information that I can use in my everyday systems administration and systems engineering roles. *Windows IT Pro* magazine has provided me with a wealth of information for over 10 years." —Gary T. Systems Specialist
"Lots of unique information using real-world scenarios" —B. P. Senior Systems Analyst
"The only magazine I get in print, so if I'm busy, I can read the issue later. This is one I never miss reading an issue." —R. Z. VP Microsoft Practice
But don't take our word for it! Read our magazine or check out our web site today! Keep the discussions going by posting blogs, commentary, videos and more.
www.windowsitpro.com
Windows IT Pro

Using IPsec to Isolate Servers in Windows Server 2008 and Windows Vista

by Damir Dizdarevic

The primary purpose of IPsec is to protect the content and integrity of network traffic by implementing digital signing and encryption. But when you need to restrict access to certain resources, you probably turn to Access Control Lists (ACLs) or VLANs as the most likely candidates for this purpose. But ACLs—specified in the application layer—can end up posing a great security risk. In reality, you can use IPsec for the purpose of isolating specific hosts or domains from the threat of unauthorized (or unmanaged) computers.

In particular, the new IPsec-based Connection Security Rules in Windows 7, Windows Server 2008, and Windows Vista—configurable through the Windows Firewall with Advanced Security Console and Group Policy—provide an excellent tool for implementing server isolation. Let's start with a little background about server isolation in general, then dive into the process of configuring it in your environment.

What Is Server Isolation?

By implementing server and domain isolation, you propagate a network policy that requires that specific servers—members of a domain—accept authenticated and secured communications only from other domain-member computers. This network policy isolates specific servers from computers that aren't domain members, or computers that are domain members but don't satisfy certain criteria. For example, you can configure a policy that forces a database server to accept connections only from the servers that are members of a specific security group or that have a certain computer certificate installed.

When you implement isolation this way, there's no need to reconfigure the network or implement any third-party software. Everything you need is already present in the OS. Hosts or domains isolated in this way will require no maintenance in case of changes in network design or migrations to another location or another network device. Because isolation is implemented at the OS level, it won't interfere with other levels of protection.

In Windows Server 2003, server isolation was possible by configuring the *Access this computer from network* Group Policy setting, but this feature's functionality was limited. It was possible only to grant users or computers the right to access a specific host; you couldn't assign additional options such as the

Connection Security Rules integrate IPsec and firewall functionality for the first time

authentication method. Also, it was possible to force an authentication protocol through Group Policy (e.g., to accept only NTLMv2), but it wasn't possible to force Kerberos or to request certificates for authentication.

Windows 7, Server 2008, and Vista provide new functionalities for server isolation through the Windows Firewall with Advanced Security Console. Aside from providing advanced firewall configuration possibilities, this console lets you implement Connection Security Rules. These rules are crucial for the implementation of server isolation. Although IPsec-based isolation was possible in earlier OSs such as Windows XP and Windows 2003, Server 2008 and Vista integrate IPsec and firewall functionality for the first time.

Requesting or Requiring?

Your first task is to identify the host you want to isolate, then determine the level of isolation to implement. In some cases, server isolation will occur on all hosts in a domain, which essentially equates to domain isolation. However, more often, you'll want to isolate specific (client or server) machines that require an additional layer of security. So, let's focus on implementing isolation on a single host. (Because Connection Security Rules exist on both Vista and Server 2008, and are configured the same way, I won't focus on a specific OS.)

You'll find the Windows Firewall with Advanced Security Console in the Control Panel Administrative Tools applet. After you open the console, which Figure 1 shows, right-click the Connection Security Rules node and select New Rule. Doing so starts the New Connection Security Rule Wizard, which offers several choices. Choose the first option, Isolation. The other available options let you make an exemption rule for specific hosts, implement authentication between two specific computers (the Server-to-Server option), force authentication in tunneling mode (useful for site-to-site links), or make a custom rule.

After you select Isolation and click Next, you must choose

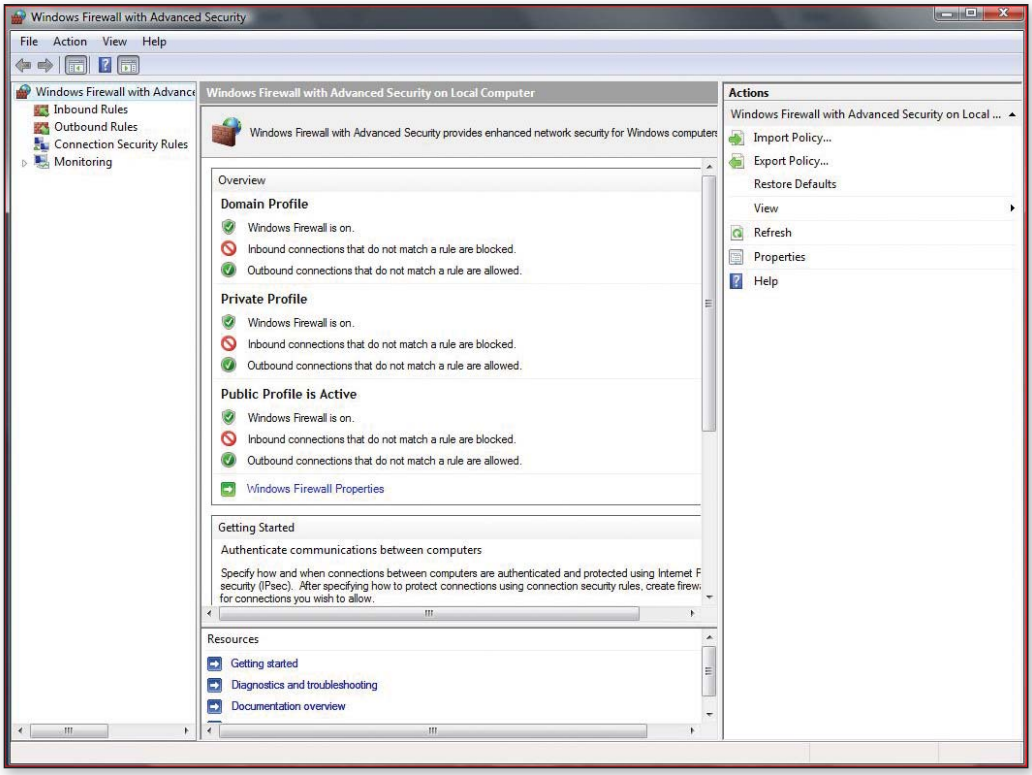


Figure 1: The Windows Firewall with Advanced Security Console

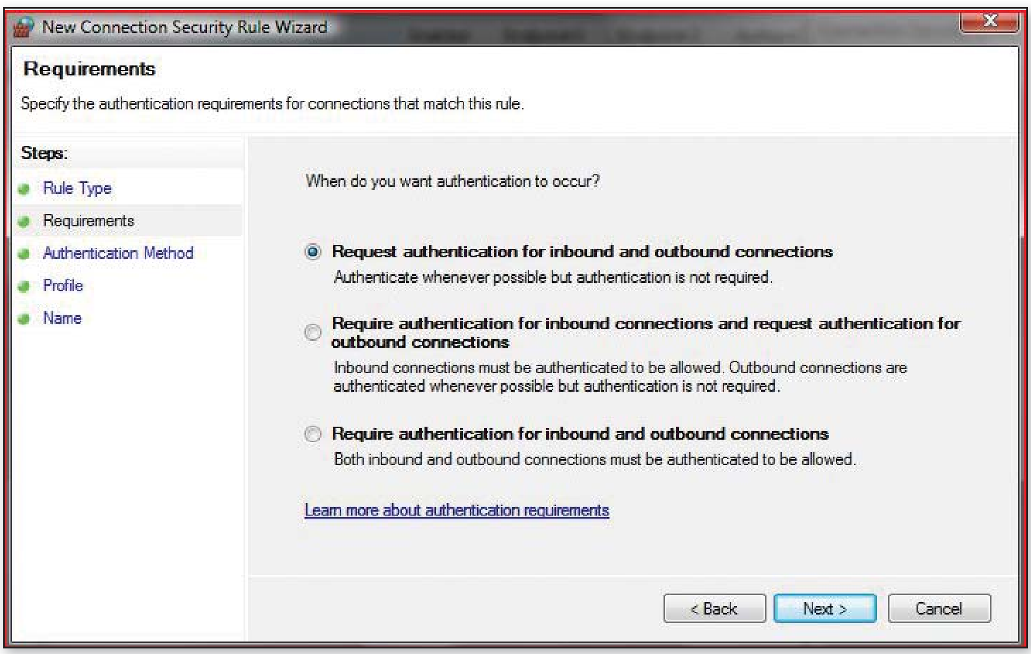


Figure 2: Choosing between requesting and requiring

between several authentication requirements, as you see in Figure 2. Essentially, your choice is between *requesting* and *requiring*. If you choose a Request option, authentication will be requested (i.e., offered) for inbound or outbound traffic (or both), but it won't be forced. If the other party can't properly authenticate, traffic will still be allowed. If you choose a Require option, the OS will force authentication and will drop the connection if authentication is unsuccessful. Depending on your required level of security, you can choose *Require authentication for inbound connections and request authentication for outbound connections,* which is acceptable if you want only to force inbound authentication (when other hosts are trying to access this isolated host), or you can choose *Require authentication for inbound and outbound connections,* which maximizes security by forcing authentication on both inbound and outbound traffic.

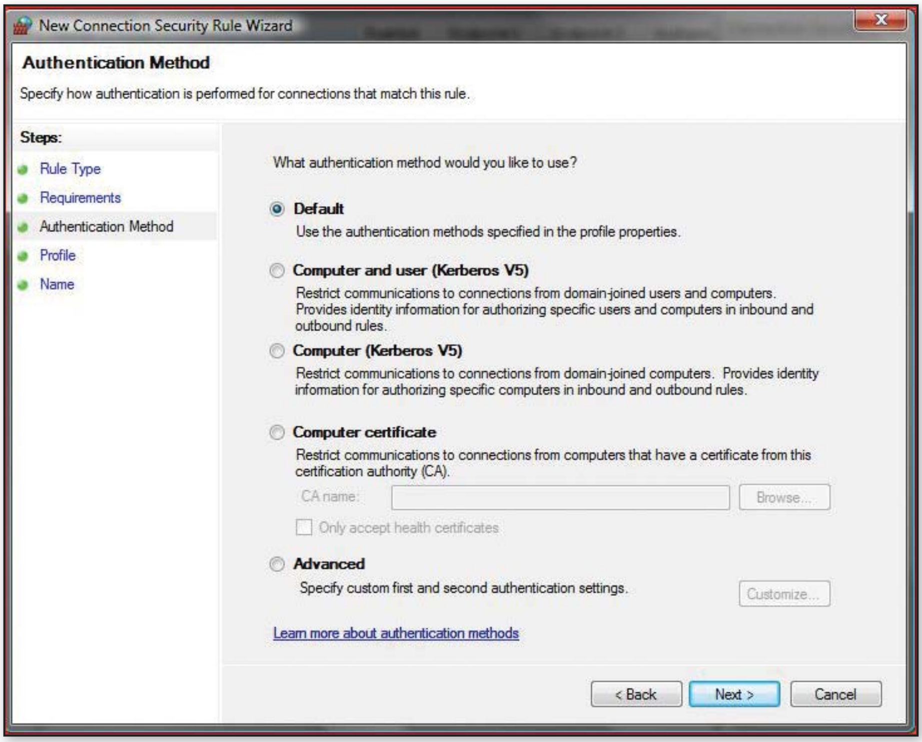


Figure 3: Configuring an authentication method

The first option, *Request authentication for inbound and outbound connections*, won't force authentication in any way, so it's not true isolation. The second option, *Require authentication for inbound connections and request authentication for outbound connections*, will keep an acceptable level of security for an isolated host while still allowing the host to communicate with all other hosts (domain and non-domain). For that reason, the second option is a good solution, so select it and click Next.

Configuring Authentication

Next, you need to configure an authentication method, as Figure 3 shows. In this step, you can actually force Kerberos authentication for a user, a computer, or both; require certificates; or implement a custom authentication method. However, you should be aware that these authentication mechanisms are mandatory at the IPsec level (i.e., the network layer). If some application uses another method of authentication (e.g., NTLM), authentication will occur again at the application layer. If you select the default option, authentication will be implemented as configured on the *Windows Firewall with Advanced Security Properties* dialog box's IPsec Settings tab. To access these settings, right-click the *Windows Firewall with Advanced Security on Local Computer* node and select Properties. On the IPsec Settings tab, you can select Customize to configure the values that will be treated as defaults during the creation of new connection security rules, as Figure 4 shows.

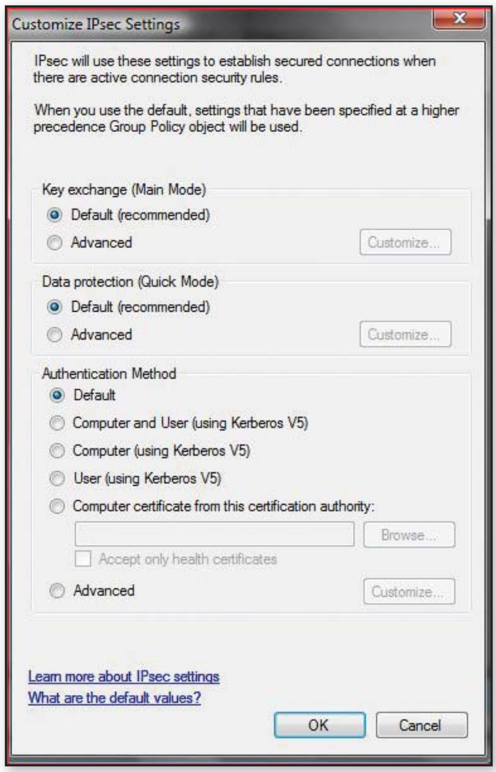


Figure 4: Customizing IPsec settings

Computer and user. If you select the second Authentication Method option, *Computer and User (using Kerberos V5)*, every connection attempt to an isolated host will require Kerberos authentication. If both the user and computer are domain members, authentication will occur automatically, requiring no user intervention. This authentication method is easy to implement and provides a high level of security, so I recommend it for most scenarios.

Computer. If you select the *Computer (using Kerberos V5)* option, authentication will be required only from the computer. In other words, if the computer that's initiating a connection to the isolated host is a domain member, the connection will be permitted without requiring any kind of user authentication.

Computer certificate. The *Computer certificate* option—the most restrictive—lets you specify that only computers that have a

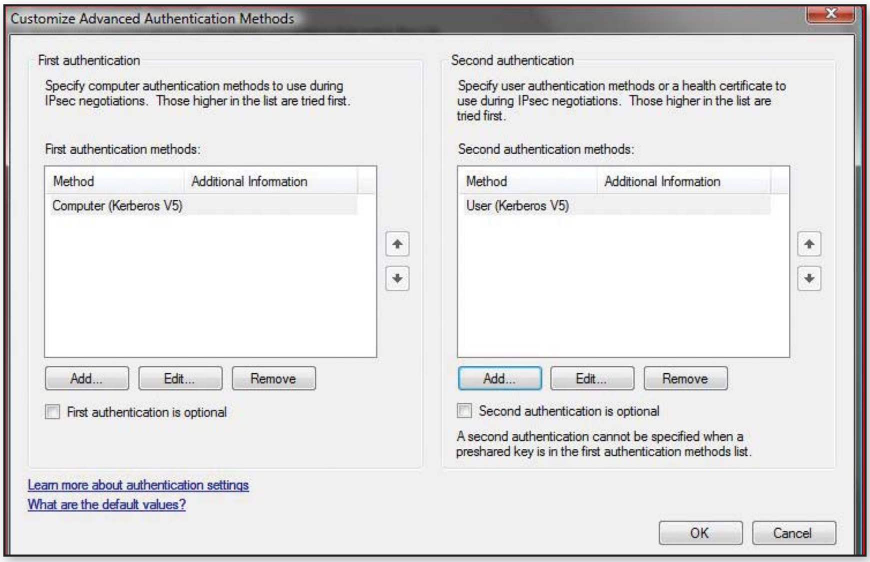


Figure 5: *First authentication* and *Second authentication*

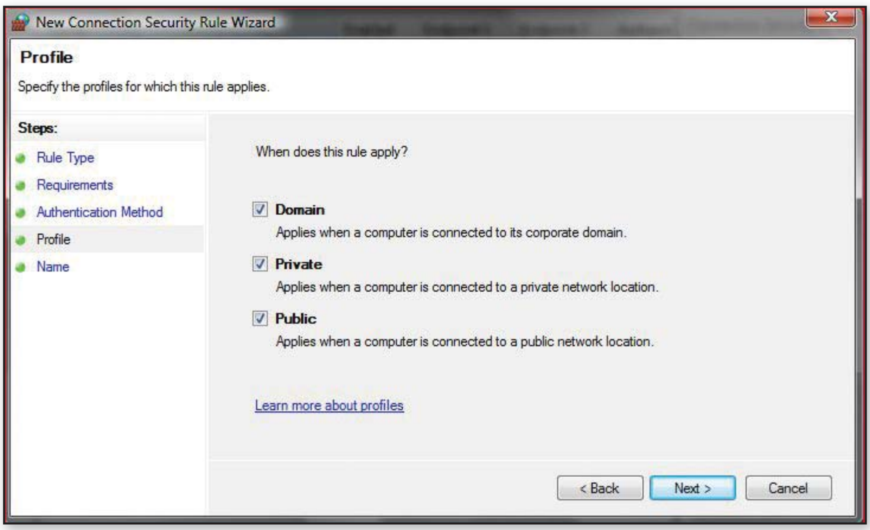


Figure 6: The wizard's Profile page

certificate issued by a specific Certification Authority (CA) can access the isolated host.

Health certificates. Near the bottom of the Customize IPsec Settings dialog box is an interesting check box called *Accept only health certificates,* which can add an additional level of security. If IPsec is used in combination with NAP for unhealthy host isolation, the isolated host will accept only computer certificates that are issued by the Health Registration Authority component of the NAP solution. For more information about configuring NAP with IPSec, see the Microsoft article "Step-by-Step Guide: Demonstrate NAP IPsec Enforcement in a Test Lab" (www.microsoft.com/Downloads/details.aspx?FamilyID=298ff956-1e6c-4d97-a3ed-7e7ffc4bed32).

Advanced. At the bottom of the dialog box, you'll see an Advanced option, which lets you select various authentication methods that are performed during the negotiation and security association phases of IPsec. A security association is a combination of a negotiated key, a security protocol, and a security parameters index, which together define the security used to protect the communication between hosts. When you click Customize, a new window presents twin dialog boxes called *First authentication* and *Second authentication,* as Figure 5 shows.

The first authentication method occurs during the Main Mode phase of IPsec negotiations. In this phase, the two computers establish a secure, authenticated channel by going through policy negotiation, a Diffie-Hellman exchange, and authentication. With the second authentication method, you can specify how the user who is logged on to the peer computer authenticates. Available choices are the Kerberos V5 authentication protocol, user certificates, and a computer health certificate. Both are optional, but for a secure environment, you should require at least first authentication. For the purposes of this article, select the *Computer and User (using Kerberos V5)* authentication method and click Next.

Which Network Profile?

On the wizard's Profile page, which Figure 6 shows, you can determine which network profile this rule applies to. Your choices are Domain, Private, and Public, and they're all selected by default. However, you should consider changing these values, particularly if you're frequently changing the location of the isolated host (e.g., laptop computers). The Domain network profile refers to a network that lets you connect to your domain controllers (DCs) and log on to the domain. The Private profile applies to networks that the user marks as Private (e.g., home networks). The Public profile applies to networks that the user marks as Public after he or she connects to them (e.g., networks with a high security risk, such as networks in hotels and public hot spots).

In some cases, you'll want to clear the Private check box. For example, if you're implementing a Connection Security Rule for your laptop, you'll probably want to isolate it in a domain or a public environment but retain access in your home (private) network. Of course, for maximum security, all options should remain selected.

The final step in the wizard is to give the rule a name. I recommend using a descriptive name. After you click Finish, the rule will be automatically activated and will appear in the list of rules.

Implementing Firewall Inbound Rules

If you want to further restrict communication to the isolated host, you can configure additional firewall inbound rules—for example, specifying the ports that are opened for communication and the IP addresses from

which communication will be possible. Although you can do this by using just IPsec or pure networking technologies, the new Windows Firewall with Advanced Security Console lets you control it from single place. Also, you can require the implementation of encryption for traffic security by implementing Encapsulating Security Payload (ESP) through the Windows Firewall with Advanced Security Console.

Right-click the Inbound Rules node, and select New Rule to start the New Inbound Rule Wizard. Select Port, click Next, choose between TCP or UDP, and specify the port that you want to open (for example, you can open only ports for web traffic, 80 and 443). Click Next. On the next screen, select the *Allow the connection if it is secure* option, as Figure 7 shows. Doing so essentially connects this rule with the Connection Security Rule you already created. (Connections through the ports you specify here will occur only if they're authenticated through a Connection Security Rule.) To implement traffic encryption, you can also select the *Require the connections to be encrypted* option. Click Next, and you can specify the computers and users (domain members) to which this rule applies. Finally, you can choose a network profile and name the rule.

For more information about configuring firewall rules, see the Microsoft article "Windows Firewall with Advanced Security and IPsec for Windows Server 2008" (technet.microsoft.com/en-us/library/dd448524.aspx).

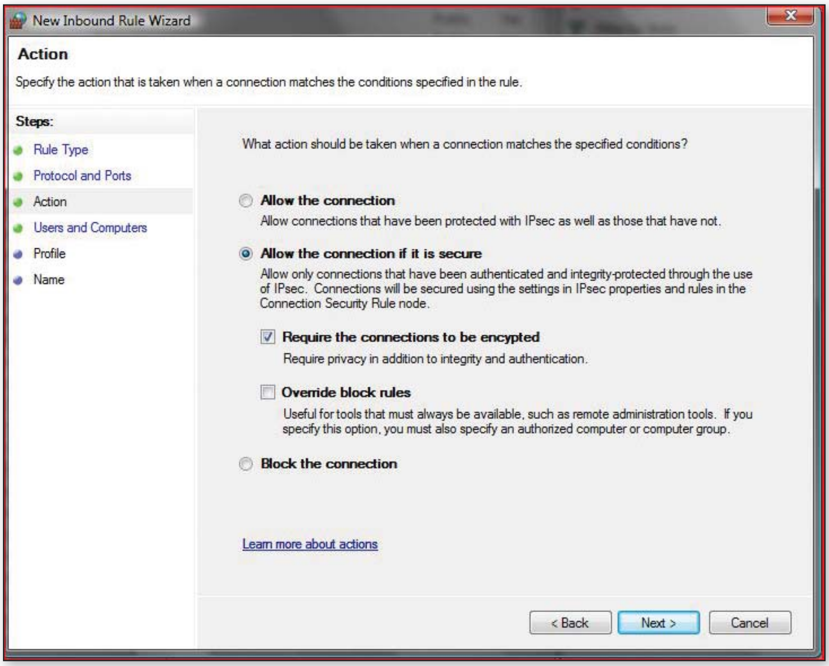


Figure 7: The New Inbound Rule Wizard

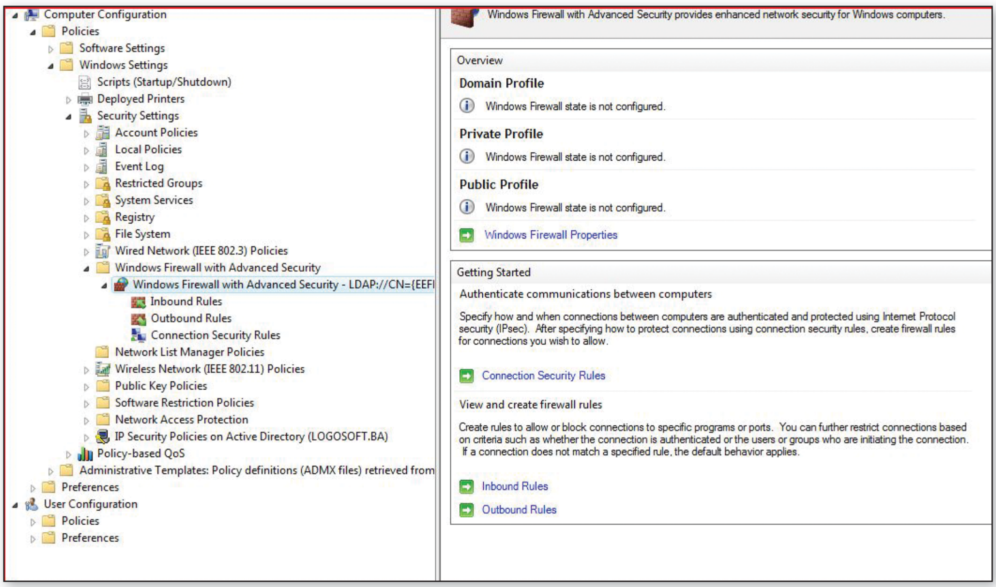


Figure 8: Using Group Policy

Configuring Exemptions

In some situations, you'll want to exempt computers, groups, or ranges of IP addresses assigned to computers from being required to authenticate when initiating a connection to an isolated host—regardless of other Connection Security Rules.

For example, you might use exemption to grant access to infrastructure computers (e.g., AD DCs, DHCP or CA servers) that the isolated host must communicate with before authentications can be performed.

A word of warning: Be very careful configuring isolation rules that can affect infrastructure servers. CA, DC, DHCP, DNS, and other infrastructure servers shouldn't have any requirement for IPsec communication for inbound or outbound connectivity. If rules are created, they should be crafted extremely carefully so that unauthenticated computers can authenticate and get access to these services. Member servers and workstations should be configured to neither request nor require authorization to those servers, and the exception rules should be used to configure that.

To configure exemption, start the New Inbound Rule Wizard again by right-clicking Connection Security Rules, then select Authentication Exemption and click Next. On the next screen, you can click Add to add computers, IP ranges, or specific computer types that will be exempted from authentication. When you make your choice, click Next and select the network profile that this rule will apply to. Then, name the rule and click Finish.

Using Group Policy

The most convenient way to enable server isolation on several computers is through Group Policy. To do so, you need to have Server 2008 DCs because these options aren't available in Windows 2003 Group Policy objects. However, if you have Windows 2003 DCs, you can still use IPSec policy options.

Before creating and linking a Group Policy Object (GPO), you should group hosts with the same isolation requirements into separate organizational units (OUs). After you've created an OU structure and moved servers to their proper OUs, open the Group Policy Management Console from Administrative Tools. Create a new GPO inside the Group Policy Objects container, right-click it, and select Edit to open it. Navigate to the Computer Configuration node, and expand Policies, Windows Settings, Security Settings, Windows Firewall with Advanced Security. In the Group Policy Management Editor's right pane, you'll see the same UI you'd see if you were running this console locally, as you can see in Figure 8, page 43. Click Connection Security Rules, start the New Inbound Rule Wizard, and implement your desired options as I described earlier.

After you finish, you'll have a Connection Security Rule created inside the GPO. If you right-click the rule, select Properties, and go to the Computers tab, you can specify rule endpoints—computers to which this rule will apply. You can specify one or more computers as either endpoint. You can specify a specific IP address, a subnet, a predefined address, or an IP address range. Be aware that the Connection Security Rule will apply to communications between any computer in Endpoint 1 and any computer in Endpoint 2. After you configure all necessary options, you can link the GPO to the OU that contains the hosts that need to be isolated.

Complementary Security

Server isolation provides an extra layer of security and access control that complements other security technologies such as antivirus, anti-spyware, firewall, and intrusion detection system (IDS) solutions. It lets you use Group Policy settings to create, distribute, and centrally manage Connection Security Rules to isolate specific hosts.

This solution also results in a zero-touch deployment experience and an unchanged experience for end-users. No additional end-user training is necessary, and there's no need to install new software or visit each computer during deployment—a great benefit of this technology!

InstantDoc ID 103088

Damir Dizdarevic (ddamir@logosoft.ba), manager of the Learning Center at Logosoft in Sarajevo, Bosnia, has published more than 380 articles in various IT magazines. He's an MVP for Windows Server Infrastructure Management, and an MCSE, MCTS, MCITP, and MCT.

Solving PowerShell Argument Input Errors with WRAPPER SCRIPTS

by Alex K. Angelopoulos

Here are 3 solutions for correctly passing strings with embedded spaces into PowerShell scripts

As a security measure, Windows PowerShell doesn't create an association between the script extension .ps1 and the PowerShell command shell. The result is that clicking on a file with the extension of .ps1 doesn't cause it to execute, and you can't just drag and drop files onto a PowerShell script icon for easy execution. You can create a Windows shortcut or a Cmd.exe batch file that wraps up the process of invoking PowerShell explicitly for a script. This workaround doesn't represent a security problem in itself because it doesn't create the vulnerabilities that a file-type association does. However, due to the way arguments are parsed and passed on by Windows, arguments that need to be enclosed in quotes (e.g., they include spaces) aren't passed correctly to PowerShell scripts.

Fortunately, there are several ways around this problem; the most common ways involve a batch-file wrapper, which I refer to as a *wrapper script* for simplicity. I'll explain the problem and the basic workarounds, as well as some points that might be important if you need to go further than I do here.

The Problem: Stripping Double Quotes

The easiest way to communicate the problem is to use an example. We start out with a simple PowerShell script, echodemo.ps1, which looks like this:

```
#echodemo.ps1
$i = 0;
foreach($arg in $args)
{$i++; "$i $arg"}
```

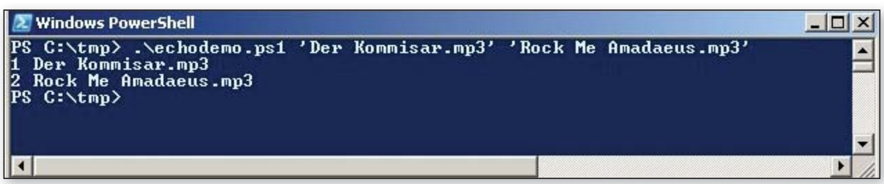


Figure 1: Sample of Echodemo.ps1 running, with output

All this script does is loop through each of the arguments passed to it, writing an argument counter and the argument for each one. For ease of testing, I have the script saved in the same folder as a couple of files that have spaces in their names. As Figure 1 shows, when I run the script with the filenames as arguments, the script treats each quoted string as a separate argument.

PowerShell lets you specify command-line options when you start PowerShell, and by using the Command option, you can explicitly tell PowerShell to run a script or an internal command. You can see the detailed Help for PowerShell's command-line options by entering the following command at either a Cmd.exe or PowerShell.exe prompt:

```
powershell -?
```

We want to run commands that need command-line parameters passed into PowerShell. According to the PowerShell 1.0 Help documentation, we just need to use

```
powershell -Command
```

followed by a script block. This works fine—as long as there are no quotes needed for filenames or other parameters passed into PowerShell. If this sounds confusing, don't worry: In fact, it's simpler to run commands than the Help information indicates.

We're aided in the search for a solution by the fact that Cmd.exe command shell scripts have a special generic placeholder variable, %*, that substitutes in all unused arguments, putting quotes around them as needed. However, this process doesn't correctly run all commands in PowerShell. Listing 1 shows several Cmd.exe wrapper scripts I wrote to demonstrate how %* variable expansion works. These examples will let us explore what happens when you create a Cmd.exe wrapper script for running a PowerShell script that takes multiple quoted arguments.

Figure 2 shows the output from the first four scripts in Listing 1. The output from wrapper0 clearly shows that %* expansion substitutes the filenames, with quotes as needed. The wrapper1 script doesn't cause echodemo.ps1 to run at all; instead, it appears that PowerShell interprets everything within the script block brackets as a single string, and PowerShell simply echoes back what it received. In wrapper2, I include the PowerShell invocation operator, &, and quote the entire string. Now echodemo .ps1 runs, but the quotes are stripped from the quoted arguments. As a result, each word of each filename is interpreted as a separate argument. In wrapper3, I make a last-ditch attempt, which I knew would fail, quoting the argument expansion term %*. This method concatenates all of the command-line arguments into a single long argument.

So how do we pass data containing embedded spaces into PowerShell? We actually have our choice of solutions, and that's what the rest of this article is about.

SOLUTION 1: PowerShell 2.0's File Parameter

PowerShell 2.0, which is in its Community Technology Preview (CTP) stage as I write, provides an alternative string parsing technique for running a script. You can use -File instead of -Command, followed by the path to the script and the arguments you wish to use with the script, and the arguments will be parsed correctly. So with PowerShell 2.0, we can use a batch-file wrapper such as the following command, which is also shown as wrapper4.cmd in Listing 1:

```
PowerShell -File echodemo.ps1 %*
```

PowerShell passes the arguments following the script path directly to the script as the pre-parsed $args array. The result is that each quoted argument appears as a separate argument. Of course, this method works only if you have PowerShell 2.0 installed. You can download the CTP3 version from the Microsoft Download Center at www.microsoft.com/downloads/details .aspx?FamilyID=c913aeab-d7b4-4bb1-a958-ee6d7fe307bc.

However, telling someone they need to upgrade is one of the top 10 most irritating responses to a technical problem, so let's explore how you solve this problem with PowerShell 1.0.

SOLUTION 2: Turn Arguments into PowerShell 1.0 Input

To increase PowerShell's flexibility, you can use a hyphen (-) following the Command parameter to tell PowerShell to interpret input as command text to execute. In a batch file, this technique means you can

```
C:\WINDOWS\system32\cmd.exe

C:\tmp>wrapper0 "Der Kommisar.mp3" "Rock Me Amadaeus.mp3"

C:\tmp>echo "Der Kommisar.mp3" "Rock Me Amadaeus.mp3"
"Der Kommisar.mp3" "Rock Me Amadaeus.mp3"

C:\tmp>wrapper1.cmd "Der Kommisar.mp3" "Rock Me Amadaeus.mp3"

C:\tmp>powershell -Command { .\echodemo.ps1 "Der Kommisar.mp3" "Rock Me Amadaeus.mp3" }
.\echodemo.ps1 Der Kommisar.mp3 Rock Me Amadaeus.mp3

C:\tmp>wrapper2.cmd "Der Kommisar.mp3" "Rock Me Amadaeus.mp3"

C:\tmp>powershell -Command "& {.\echodemo.ps1 "Der Kommisar.mp3" "Rock Me Amadaeus.mp3" }"
1 Der
2 Kommisar.mp3
3 Rock
4 Me
5 Amadaeus.mp3

C:\tmp>wrapper3.cmd "Der Kommisar.mp3" "Rock Me Amadaeus.mp3"
1 Der Kommisar.mp3 Rock Me Amadaeus.mp3

C:\tmp>_
```

Figure 2: Output from the first four scripts in Listing 1

pipe anything, including the output of an echo command, into PowerShell and it will be received without any further parsing or quote-stripping by Windows or Cmd.exe. The wrapper5.cmd batch file shown in Listing 1 uses this technique to make PowerShell correctly interpret quoted arguments.

By the way, PowerShell automatically exits after it finishes the script when you use wrapper5.cmd. This behavior is desirable if you're using the script to accomplish a task directly. However, if you want to inspect the output from the PowerShell script, you'll want to use PowerShell's NoExit parameter, as shown in wrapper6.cmd in Listing 1.

This technique also works in the PowerShell 2.0 CTP releases, so it should be fully forward-compatible. However, it still has one basic flaw. Many of PowerShell's special characters are used in variant but regrettably common filenames. Names that contain parentheses in particular can cause PowerShell to attempt evaluating the content as an embedded command. To solve such problems, we need a better way to handle passing commands to PowerShell.

Listing 1: Cmd.exe Wrapper Scripts that Demonstrate %* Variable Expansion

```
::wrapper0.cmd
:: Just expands and echoes arguments to standard output
echo %*

::wrapper1.cmd
:: Everything inside {} is echoed as a string
powershell -Command { .\echodemo.ps1 %* }

::wrapper2.cmd
:: Double quotes are stripped out completely
powershell -Command "& {.\echodemo.ps1 %* }"

::wrapper3.cmd
:: Expanded arguments become one string in '%*'
powershell -Command "& {.\echodemo.ps1 '%*' }"

::wrapper4.cmd
:: Works properly - PowerShell 2.0 only
powershell -File .\echodemo.ps1 %*

::wrapper5.cmd
:: Input processed as a command; works in PowerShell 1.0 and 2.0
echo .\echodemo.ps1 %* | powershell -Command -

::wrapper6.cmd
:: As wrapper5.cmd, but -NoExit keeps PowerShell running
echo .\echodemo.ps1 %* | powershell -NoExit -Command -
```

Telling someone they need to upgrade is one of the top 10 most irritating responses to a technical problem, so let's solve this problem with PowerShell 1.0.

We need to process items so that PowerShell unambiguously treats them as file and folder names as well. Therefore, we'll need a stronger solution than a batch-file wrapper. Our last solution uses VBScript to correctly pass arguments to PowerShell.

SOLUTION 3: Using a WSH Wrapper Script

Listing 2, page 48, shows a generic Windows Script Host (WSH) wrapper script that you can use as a drag-and-drop wrapper for any PowerShell script. To prepare the wrapper script, simply use the following steps:

1. Save a copy of the VBScript template to the same folder as the PowerShell script you wish to run, and make sure the basename (the bare name of the file) of the VBScript file is identical to the basename of the PowerShell script. For example, if the PowerShell script is C:\apps\Scan-File .ps1, its basename is Scan-File. So you would save the VBScript template as C:\apps\Scan-File.vbs. The VBScript wrapper can then figure out what the name of the PowerShell script is.

2. The VBScript wrapper runs the PowerShell script so that it automatically exits and closes when it's finished running. If you want to keep the PowerShell script running, go to the area in the script file where the base command is defined, callout A, and comment it out by inserting an initial single quote (VBScript's single-character comment marker). Then remove the initial single quote commenting out the base definition in callout B. If you want the script to go away when it finishes running, however, leave things as they are.

3. The VBScript wrapper runs the PowerShell script in a minimized window to make it as unobtrusive as possible. If you prefer to run the script with the PowerShell window appearing differently, go to callout C, the line that reads *WshShell.Run Command, 2*. The final numeral controls the window style. To run the window with the default output position and size, which is useful if you're going to look at output from the script or if it might prompt you for additional information, change the 2 to a 1. If the script doesn't prompt you for anything and doesn't display any output you need to see, you can change this number to 0, which keeps the window hidden. Choose this option only if you aren't keeping PowerShell running using the code in callout B. Keeping the session running combined with running the PowerShell window hidden means that each time you use the script, you'll have a new, hidden PowerShell session that continues to run until you reboot or end the process from Task Manager.

4. If you like, create a shortcut to the WSH script on your desktop for easy access.

To use the PowerShell script, just drag and drop files and folders onto the WSH script or your shortcut to it. The script locates the PowerShell script based on the assumption that the PowerShell script uses the same name as the WSH script and is in the same folder, then starts assembling a command line for executing the PowerShell script.

Listing 2: Generic WSH Wrapper Script for any PowerShell Script

```
' BEGIN WSH wrapper script
' Should have same basename as PS script it will run,
' and must be in same folder as PS script.
' ex: if c:\tmp\fred.ps1, this must be c:\tmp\fred.vbs

dim fso: Set fso = CreateObject("Scripting.FileSystemObject")
Dim WshScript: WshScript = WScript.ScriptFullName
Dim PsScript
PsScript = fso.BuildPath( _
    fso.GetFile(WshScript).ParentFolder.Path, _
    fso.GetBaseName(WshScript) & ".ps1")

' Escape spaces embedded in script path, if any.
PsScript = Replace(PsScript, " ", "` ")
' Escape single quotes by doubling.
PsScript = Replace(PsScript, "'", "''")


Dim i, arg
i = 0
Dim ArgSet: Set ArgSet = CreateObject("Scripting.Dictionary")
Argset(i) = PsScript

For each arg in WScript.Arguments
  ' EXPLICITLY ensure these resolve to file/folder paths
    if fso.FileExists(arg) or fso.FolderExists(arg) then
        i = i + 1
        ' Include escapes for singlequotes in paths, if any
        Argset(i) = "'" & Replace(arg, "'", "''") & "'"
    End If
Next

Dim base

A base = "PowerShell -Command ""& {"

' Use the following base instead to keep the window open.

B 'base = "powershell -NoExit -Command ""& {"

Dim Command

Command = base & Join(ArgSet.Items) & "}"""

' WScript.Echo "command as passed to PowerShell:", Command
Dim WshShell: Set WshShell = CreateObject("WScript.Shell")

' Now run the command

C WshShell.Run Command, 2

' END WSH Wrapper Script
```

First, the VBScript code makes sure any spaces in the path to the script are escaped so that PowerShell won't interpret the name as multiple arguments. Next, the script loops through the names of items dropped onto it. VBScript checks to ensure that each item is a real file or folder, discarding it otherwise. After the item is confirmed as a file-system item, VBScript checks for single quotes used as part of the filename and escapes them for PowerShell. Next, the name is surrounded with single quotes and saved in the collection of prepared arguments. When all arguments have been processed, the script assembles them into a PowerShell-safe command statement and runs it.

This process might seem like overkill for this kind of problem, but it's actually a reasonable solution. Other scripting languages occasionally make similar accommodations; for example, Perl uses similar batch files as wrappers for Perl scripts designed to run from a command prompt, and those batch scripts can sometimes be hundreds of lines long. When you know how you typically run your PowerShell drag-and-drop scripts, you won't even have any customization to do. All you'll generally have to do is copy your template and rename it to match your next PowerShell script that you want to use this technique with.

Choosing a Solution

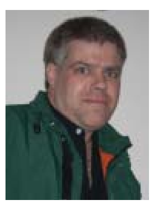
Deciding which technique to use for making batch-file wrappers to pass quoted strings correctly to PowerShell is straightforward for most problems. If you can use PowerShell 2.0—when it's available—running Powershell.exe with the File parameter is a good solution to the problem because it correctly parses quoted filenames and other quoted input arguments. If for some reason you can't use PowerShell 2.0, and if your need is primarily drag-and-drop processing, a batch file wrapper written like wrapper5.cmd or wrapper6.cmd should do the trick. If you need Cmd.exe and PowerShell interoperability, you can use wrapper2.cmd with explicit single quoting where needed, or (preferably) work from PowerShell as your default command shell.

For drag-and-drop use, all you need to do is create the appropriate wrapper script in the same folder as the PowerShell script you want to use as your drop target; the resulting script should look like my wrappers, but with the name of your script substituted for echodemo.ps1.

The solutions should work for most scenarios, but there are situations where you might have trouble. PowerShell makes copious use of special characters that are occasionally also used in filenames. Those special characters that can cause odd behavior in specific situations include all of the brackets and parentheses, as well as $, `, and '. Although it's possible to escape these characters so that PowerShell handles them correctly, it would be a complex job. This kind of task is best performed from a WSH wrapper script that explicitly parses an entire command sequence and escapes it before passing it on to PowerShell.

The scripts in this article are available for download from *Windows IT Pro*'s website. (Go to www.windowsitpro.com, enter 103174 in the InstantDoc ID text box, then click the *Download the Code Here* button.) For most uses, you should find that wrapper scripts 2, 5, and 6 work as templates for drag-and-drop PowerShell wrapper scripts that correctly handle filenames with embedded spaces.

InstantDoc ID 103174



Alex K. Angelopoulos
(aka@mvps.org) is an IT consultant, an MCSE, and a contributing editor for *Windows IT Pro*. As an avid scripter, he regularly writes about administrative automation using WSH, PowerShell, and related technologies.

SharePointPro 2010 SUMMIT & EXPO

The Top Reasons to Attend

- Celebrate the upcoming release of Sharepoint 2010 with members of the teams that built the products.
- Find out from industry insiders the best migration path if your company is considering an upgrade.
- Listen to Microsoft discuss the many enhancements and new features of SharePoint 2010.
- Find products and services from our partners in the Expo Hall that can save money, save time, and help your business do more.
- Book your hotel early and take advantage of GREAT hotel rates at the world famous Bellagio. Reserve your room at the Bellagio by the early bird date and get a $100 Bellagio certificate.
- A strong network of peers is an invaluable resource; build yours with the unparalleled networking opportunities at the conference. Come prepared to meet and interact with people at other companies and take advantage of their experiences.
- Unwind in Vegas and make new friends! You know what they say about Vegas…
- Impress your boss and colleagues. You'll go back to the office with practical tips and tricks that will make development, deployment, and administration of your SharePoint solutions faster and easier.
- Enjoy the excitement and luxury of one of Las Vegas' premiere hotels. Enjoy some of the best dining in the culinary world, famous Vegas shows, fine shopping, the famous fountains of the Bellagio, the gallery of fine art, the World-famous Shadow Creek golf course and the 24/7 buzz of the casino.

SCHEDULE at a Glance

TUESDAY, MARCH 16, 2010	
7:30 am - 5:00 pm	Conference Registration
9:00am - 4:00 pm	Pre-conference Workshops
WEDNESDAY, MARCH 17, 2010 MICROSOFT DAY	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:00 am - 9:00 am	Keynote
9:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 5:00 pm	Expo Hall Open
THURSDAY, MARCH 18, 2010	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 4:00 pm	Expo Hall Open
FRIDAY, MARCH 19, 2010	
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 11:30 am	Conference Sessions

Microsoft Day

SAMPLING OF SESSIONS PRESENTED BY MICROSOFT SPEAKERS.

Please check Web site as we add more sessions that are currently under NDA.

DEVELOPER

HMS01: OVERVIEW OF MICROSOFT SHAREPOINT 2010 FOR THE DEVELOPER
MICROSOFT

HMS02: INTRODUCTION TO SHAREPOINT DEVELOPMENT WITH VISUAL STUDIO 2010
MICROSOFT

HMS03: DEVELOPING BUSINESS INTELLIGENCE SOLUTIONS WITH SHAREPOINT 2010
MICROSOFT

HMS04: DEVELOPING INTERNET-FACING SITES USING SHAREPOINT 2010
MICROSOFT

HMS05: ENHANCING THE SHAREPOINT 2010 USER EXPERIENCE THROUGH SILVERLIGHT
MICROSOFT

HMS06: DEVELOPING ENTERPRISE APPLICATIONS USING THE BUSINESS CONNECTIVITY SERVICES
MICROSOFT

HMS07: EXTENDING THE ENTERPRISE SEARCH EXPERIENCE IN SHAREPOINT 2010
MICROSOFT

IT PRO

HMS08: UPGRADING FROM SHAREPOINT 2007 TO SHAREPOINT 2010
MICROSOFT

HMS09: OVERVIEW OF ENTERPRISE CONTENT MANAGEMENT IN SHAREPOINT 2010
MICROSOFT

HMS10: TOP TEN SHAREPOINT 2010 FEATURES FOR THE IT PROFESSIONAL
MICROSOFT

HMS11: OVERVIEW OF HOW TO DEPLOY SOLUTIONS TO SHAREPOINT SERVER 2010
MICROSOFT

HMS12: INTRODUCTION TO SHAREPOINT 2010 ADMINISTRATION
MICROSOFT

HMS13: WHAT'S NEW FOR SECURITY IN SHAREPOINT 2010
MICROSOFT

SHAREPOINT DEVELOPMENT

HDEV01: UPGRADING AND EXTENDING SHAREPOINT 2007 WCM SITES WITH SHAREPOINT SERVER 2010 WEB CONTENT MANAGEMENT
ANDREW CONNELL

In this session, you'll see how to upgrade a SharePoint 2007 WCM site to SharePoint Server 2010 WCM and leverage some of the new capabilities. After upgrading the site, you'll learn how to implement the ribbon and convert to the new SharePoint 2010 UI visuals. Next you'll see how to add ratings and use the content organizer.

HDEV02: INTERACTING WITH SHAREPOINT 2010 OFF THE SERVER: INTRODUCING THE CLIENT OBJECT MODEL
ANDREW CONNELL

This session demonstrates client object model, new to SharePoint 2010. This addition makes it much easier for developers to create custom solutions that leverage data stored in SharePoint from off the SharePoint server with a familiar API and without traditional Web Services. Topics covered include the .NET and Silverlight managed client object models as well as the ECMAScript object model.

HDEV03: CUSTOMIZING SHAREPOINT 2010 ENTERPRISE CONTENT MANAGEMENT DOCUMENT SETS
ANDREW CONNELL

SharePoint Server 2010 Enterprise Content Management (ECM) introduces a new concept called document sets. These enable you to create a single work product made up of multiple components. In this session, you'll learn how to create customizable document sets, custom welcome pages and much more!

HDEV04: INTRODUCTION TO SHAREPOINT DESIGNER 2010: TOP 5 GREAT THINGS TO KNOW!
ASIF REHMANI

SharePoint Designer 2010, which is a free application, is "The Preferred" tool to design powerful no-code solutions and applications in SharePoint 2010. In this session, you will get a broad overview of the capabilities of the tool, from site customizations such as modifying Site Metadata, managing Site Security, or creating Site Content, to building List- or Site-based Workflows and connecting to a variety of data sources. You will also learn about the new ribbon interface of SharePoint Designer 2010 and you'll see how best to take advantage of this application by showing the new bells and whistles that come with this product.

Sessions and speakers are subject to change. Check the Web site for details.

HDEV05: OVERVIEW: CREATING WORKFLOWS WITH SHAREPOINT DESIGNER 2010, INFOPATH AND VISIO
ASIF REHMANI

Forms and workflows are important for automating business processes. Companies usually rely on programmers to create the forms and workflows using code. Not anymore! With InfoPath 2010 and SharePoint Designer 2010, you can create powerful data-driven form composite solutions on your SharePoint sites. InfoPath gives you the ability to pull data from databases and lists, and create forms with data validation and conditional formatting. SharePoint Designer's workflows let you then design powerful multi-step workflows centered around the form collected data, building upon the out-of-the-box reusable workflows and even import workflow designs from Visio! In this session, you will see how these tools come together to design powerful end-to-end solutions on your sites.

HDEV06: GENERATE AND PUBLISH ELECTRONIC FORMS ON YOUR INTRANET USING INFOPATH 2010... NO CODE REQUIRED!
ASIF REHMANI

Finally, you can make your goals of going paperless a reality! Microsoft Office InfoPath 2010 and Forms Server 2010 come together to provide a powerful platform for electronic form generation. In this session, you will see how you can build robust electronic forms with data validation and conditional logic rules using InfoPath. Also, the inherent power of InfoPath will be demonstrated to look up data from various sources and populate it in your custom designed electronic forms. All this and more will be accomplished without writing a single line of code!

HDEV07: INDUSTRIAL STRENGTH RECORDS MANAGEMENT IN SHAREPOINT 2010
JOHN HOLLIDAY

SharePoint 2010 introduces several new document management and records management features which together represent the next generation of records management capabilities that were previously available only in the SharePoint 2007 Records Center. In this session, we'll examine document sets, persistent document identifiers, metadata-driven routing and the content organizer and we'll explore ways to apply these new features to solve traditional records management problems such as electronic record authentication and the deployment of integrated data integrity controls. During the session, we'll explore the new in-place records management features that make it easier to manage document retention schedules. You'll learn how to use con-

tent organizer rules to create detailed plans for managing how official records are organized within a given site. We'll also explore the new and improved SharePoint 2010 information management policy architecture, which includes both location-based and multiple-stage information policies, and we'll take a detailed look at the improved records center site definition to see how it simplifies the creation of a locked-down records vault.

HDEV08: PROGRAMMING BUSINESS CONNECTIVITY SERVICES SOLUTIONS IN OFFICE 2010

JOHN HOLLIDAY

SharePoint 2010 Business Connectivity Services (BCS) represents a major step in the evolution of the Business Data Catalog, with richer functionality that includes the ability to create and update back-end data, and much tighter integration with Office client applications. These new capabilities are exposed through a rich set of enhancements on both the client and the server. In this session, we'll examine both code and no-code approaches to building BCS solutions in Office 2010. First, we'll explore the new SharePoint 2010 integration features provided by the Visual Studio 2010 Tools for Office Development. Then we'll take a look at what it takes to build BCS Declarative Solutions that require no coding. During the session, we'll use the BDC client-side API to build a VSTO 4.0 add-in that integrates Line of Business (LOB) data with Microsoft Office client applications via SharePoint 2010 External Content Types and Lists.

HDEV09: EXTENDING THE VISUAL STUDIO 2010 SHAREPOINT TOOLS

TED PATTISON

The introduction of the Visual Studio 2010 SharePoint Tools really raises the bar in terms of developer convenience and productivity. And while the out-of-the-box experience with these tools goes far beyond what's been available to SharePoint developers in the past, the SharePoint Tools have been designed from the ground up to support extensibility. This session shows you how to get started by explaining how to extend the SharePoint Project System and how to use the extensibility APIs. You will learn how to create custom templates for SharePoint Projects and SharePoint Project Items (SPIs) to support common scenarios such as a solution for deploying a custom master page along with its own CCS and JavaScript files. You will also see how to extend SPIs with custom properties, context menus and event handlers.

HDEV10: SECURITY CHANGES AND ENHANCEMENTS IN SHAREPOINT 2010

TED PATTISON

SharePoint 2010 introduces a new claims-based security model that will impact the way the companies design, implement and enforce security with their SharePoint sites. This session explains the fundamental concepts of a claims-based model and shows how the new claims-based model makes it possible to use new types of security principals such as Active Directory distribution lists and SharePoint Server Audiences as first-class security objects which can be used to securely configure access to securable objects such as sites, lists, items and documents. The session will walk through developing a custom claims provider with Visual Studio 2010, which will effectively demonstrate the flexibility of how we define the people and groups from whom you need to configure access.

HDEV11: BEST PRACTICES FOR ACCESSING SHAREPOINT 2010 LIST DATA

SCOT HILLIER

In this session, attendees will learn the best ways to access and manipulate list data in SharePoint 2010. This session will begin with a discussion of server-side access using LINQ including the use of SPMetal for entity generation, writing LINQ queries against lists, and joining lists. Next, the session will present client-side access using ADO.NET Data Services through the ListData.svc service. Coverage will include using a Windows Presentation Foundation (WPF) client and a Silverlight 3.0 client. Attendees will exit the session with a strong understanding of how to utilize list data in their applications.

HDEV12: USING BUSINESS CONNECTIVITY SERVICES TO ACCESS EXTERNAL SYSTEMS WITH SHAREPOINT 2010

SCOT HILLIER

Business Connectivity Services (BCS) can be thought of as the next evolution of the Business Data Catalog (BDC) that provides a read-write capability to external data. In this session, we will cover the fundamental concepts and tools necessary to use BCS in SharePoint solutions. The session will begin by presenting the concept of an external content type (ECT) and showing how to create them in the SharePoint Designer. The ECTs will then be used to create external lists that act as a front end for a data source. Finally, attendees will learn to create a .NET Assembly Connector, which allows the creation of custom solutions for accessing external data within the BCS framework. Attendees will exit the session with a strong understanding of the BCS architecture, tools, and development practices.

HDEV13: CREATING SEARCH-BASED SOLUTIONS WITH SHAREPOINT 2010

SCOT HILLIER

Search-based solutions are applications that use a search page as the primary interface. Solutions such as image searching or travel searching in Bing are good examples of search-based solutions. SharePoint 2010 offers developers new ways to extend search and create search-based solutions. In this session, attendees will learn to create search-based solutions by using custom relevance models, extending SharePoint 2010 search parts, and utilizing .NET Assembly Connectors to access external systems. The techniques presented will prepare attendees to create search-based solutions on their own.

HDEV14: CREATING CUSTOM OFFICE BUSINESS APPLICATIONS WITH BUSINESS CONNECTIVITY SERVICES AND THE SHAREPOINT CLIENT OBJECT MODEL

TODD BAGINSKI

This session demonstrates how to build rich Office business applications which connect to data sources through the BCS and the SharePoint Client Object Model. First, the session demonstrates how to register a data source with the BCS which pulls data from multiple data sources. Then the session shows how to use the SharePoint Client Object Model to display and update the data within Microsoft Office applications. Finally, the session will demonstrate how to enhance your Office business applications even further with data stored in SharePoint lists and libraries and the SharePoint Search Service. Whether you are looking for in-depth technical knowledge about these components, or just want to get some ideas how Office business applications may be used to streamline processes and save time in your organization, this is the right session for you.

CHECK WEB SITE AS WE CONTINUE TO ADD MORE SESSIONS, SPEAKERS AND MAKE UPDATES

www.SharePointProSummit.com

HDEV15: HOW TO CREATE A YOUTUBE-LIKE APPLICATION IN SHAREPOINT WITH THE DIGITAL ASSETS LIBRARY—WITHOUT WRITING ANY MANAGED CODE!

TODD BAGINSKI

This session demonstrates how to use the new Digital Assets Library and the Videos content type to create YouTube-like functionality in your SharePoint sites. First, the session describes the new functionality the Digital Assets Library provides for videos, images, and audio files. Then the session shows how to create and configure the Digital Assets Library to display a list of videos complete with thumbnail previews. Finally, the session shows how to create a page to watch each video inside a Silverlight video player and display the details about it. All of this great functionality is implemented without writing a single line of managed code; only JavaScript, HTML, and CSS are needed to deliver the functionality!

HDEV16: SHAREPOINT 2010 DEVELOPER BEST PRACTICES

KIRK EVANS

This session will focus on best practices for developing with SharePoint 2010, including configuring a development environment, configuring application lifecycle management, unit testing, and understanding defensive development techniques.

HDEV17: DEVELOPING ADVANCED SHAREPOINT 2010 WORKFLOWS WITH VISUAL STUDIO 2010

KIRK EVANS

SharePoint 2010 includes a number of new facilities for workflow developers. Come to this session to hear about what's new in SharePoint 2010 and Visual Studio 2010 to help you code, deploy, and debug workflow solutions.

HDEV18: APPLICATION LIFECYCLE MANAGEMENT WITH SHAREPOINT 2010 AND TEAM FOUNDATION SERVER 2010

KIRK EVANS

A key part of developing for SharePoint 2010 is understanding how to work within a team of developers effectively. This requires a structured application lifecycle management process including centralized source code and build management. Come to this session to understand how to get more out of Team Foundation Server 2010 while building SharePoint 2010 solutions.

SHAREPOINT ADMINISTRATION

HITP01: DESIGNING GOVERNANCE: HOW INFORMATION MANAGEMENT AND SECURITY MUST DRIVE YOUR DESIGN

DAN HOLME

You've read the white papers, you've "Binged" governance, but how, exactly, do you design a SharePoint implementation that will support governance, security, and information management? Join SharePoint MVP and consultant Dan Holme for a practical, nuts-and-bolts look at the close relationship between your information management requirements and SharePoint's manageability controls, and the demands that relationship places on your design and infrastructure. This session is focused on architecting a logical design of SharePoint that effectively supports your information management requirements and governance plan—the "technical" side of governance. You will learn how to align your governance requirements with SharePoint farms, Web applications, and site collections. You'll discover why some third-party applications are a "design poison pill" and what SharePoint 2010 offers to greatly improve the deployment of a governable design. Gain a deeper understanding of the intricacies and challenges of designing the logical structure of SharePoint, and take away practical, blueprint-like guidance to what a governed SharePoint implementation might look like in your enterprise.

HITP02: SHAREPOINT TAKES THE GOLD IN TORINO, BEIJING AND VANCOUVER BROADCASTS

DAN HOLME

SharePoint has "won the gold" as a platform for rich collaboration and rapidly deployed solutions during the broadcast of the Olympics from Torino, Beijing and for the upcoming Vancouver 2010. Join Dan Holme, Microsoft Technologies Consultant for NBC Olympics, for an inside look at how SharePoint is put to use in one of the most unique IT efforts in the world. Discover ways that you might leverage SharePoint in your enterprise, and how the Olympics broadcast can inform the choices you make supporting and developing for SharePoint. This unique session sheds an exciting and practical light on the business value and ROI of SharePoint. Ever wonder how you can make the most of SharePoint in your organization? This session might help you figure it out!

HITP03: ENTERPRISE SOCIAL COMPUTING WITH SHAREPOINT 2010

MATTHEW MCDERMOTT

SharePoint 2010 introduces new features that support social computing for organizations of all types. Whether you have a "formal vision" or loose idea of what "social" means to your organization, this session will introduce you to the key concepts and features that can aid in your planning and implementation of social computing for your organization. This session will highlight how companies gain value out of the social computing capabilities of SharePoint.

- Introduction to the "social vision" for SharePoint 2010
- What do I like: Tagging, Rating and Notes
- What's happening: Activity Feeds
- Where is it: Social search
- Who can help: People and Expertise search

HITP04: SHAREPOINT 2010 SEARCH OVERVIEW

MATTHEW MCDERMOTT

Search has taken a huge step forward with the introduction of SharePoint 2010. This session will focus on what is new to Search in SharePoint 2010. Presented through demonstrations of the search capabilities and advancements, this presentation will provide the background necessary to understand how search has improved and how to plan for the smooth implementation of SharePoint search for your organization.

- SharePoint 2010 Search scalability options
- Improved user experience
- Social and people search
- Improved metadata processing
- Improved management and tuning

HITP05: SHAREPOINT MULTILINGUAL SCENARIOS

MATTHEW MCDERMOTT

SharePoint 2010 supports several multilingual scenarios out of the box. This session will detail the features of SharePoint 2010 that enable the creation of publishing sites that support multiple languages and locales. This session will also detail how content contributors can use the new multilingual user interface to work within their chosen language to author, manage and publish content through an interface that supports their native language. This session will detail:

- Planning a multilingual publishing site
- Implementing the multilingual user interface
- The configuration and process required for Variations
- Application of language packs
- Developer considerations for multilingual sites

HITP06: ARCHITECTING A HIGH PERFORMANCE AND FAULT TOLERANT SHAREPOINT 2010 FARM
MICHAEL NOEL

SharePoint server architecture has been significantly improved with the SharePoint 2010 wave. Gone is the inflexible Shared Services Provider, replaced by a much more scalable and fault tolerant architecture. To provide for this level of scalability, a larger number of databases and a certain level of complexity was introduced that should be understood by SharePoint architects before beginning a production SharePoint 2010 deployment. This session delves into the specifics of those infrastructure changes and demystifies many of the concepts surrounding SharePoint 2010 architecture. Best practice architectural scenarios and diagrams are illustrated and compared, and high availability options are discussed in detail.

- Learn how to architect a SharePoint 2010 for High Performance and Fault Tolerance.
- Compare and contrast best practice design examples for SharePoint deployments of varying sizes.
- Understand how to design SharePoint 2010 the right way the first time.

HITP07: BACKUP AND RESTORE FOR SHAREPOINT 2010: PROTECTING MISSION CRITICAL SHAREPOINT DATA WITH NEW TOOLS AND TECHNOLOGIES
MICHAEL NOEL

As more and more organizations use SharePoint to store documents and other critical data, it becomes imperative to provide for backup and restore specific for SharePoint. While some integrated tools exist to provide for disaster recovery, document-level restore capabilities are often needed in a SharePoint environment. This session covers some of those technologies, and focuses specifically on how the new Microsoft System Center Data Protection Manager (DPM) 2010 product can be used to provide for SharePoint-specific backup and item-level restore. In addition, specifics on how to integrate DPM with a SharePoint 2010 farm are provided and best practice architectural examples for DPM, snapshot guidelines, and deployment tips and tricks from the field are covered.

- Explore the new built in backup processes and tools in SharePoint 2010 and what should be backed up.
- Examine item-level recovery capabilities for SharePoint included in System Center Data Protection Manager.
- Learn best practice tips and tricks for deployment of DPM in a SharePoint environment.

HITP08: CONFIGURING SHAREPOINT 2010 FOR EXTRANETS
MICHAEL NOEL

SharePoint 2010 has been specifically designed to provide for a scalable and customizable environment for extranets. Infrastructure changes such as Server Groups, the services architecture, and claims-based authentication have opened the door to external deployment scenarios that were challenging with previous versions of SharePoint. This session covers extranet deployment with SharePoint 2010, focusing on alternate authentication mechanisms, scalability, and security of extranet deployments.

- Learn how to deploy extranets with SharePoint 2010 using a best practice approach to infrastructure design.
- Determine how to use claims-based authentication with SharePoint 2010 for multiple authentication sources.
- Identify how to scale SharePoint 2010 for extranet deployments.

HITP09: PROTECTING YOUR SHAREPOINT 2010 CONTENT WITH SQL SERVER 2008 TRANSPARENT DATABASE ENCRYPTION
MICHAEL NOEL

One of the "killer apps" with SQL Server 2008 is the ability to transparently encrypt all of your SharePoint content databases at the SQL level, without the need to modify any settings in the SharePoint farm. This type of transparent encryption allows organizations to comply with governmental and industry regulations that require content to be stored in encrypted format, but doesn't introduce any new complexities to a SharePoint environment, as the application itself is unaware that any encryption is happening. This session focuses on the best practices, tips and tricks, and real-world advice on how to set up and deploy SQL Server 2008 transparent database encryption for a SharePoint 2010 farm.

- Learn how to set up SQL Server 2008 for transparent encryption of content databases.
- Examine limitations, best practices, and deployment tips for implementing this new capability.
- Take an in-depth look at the security precautions and advice for the encryption methods that can be used and what makes sense for SharePoint.

HITP10: SHAREPOINT SITE LIFECYCLE-CREATING AND ARCHIVING SITES
ROBERT L. BOGUE

Managing information architecture and limiting organic site growth is a difficult issue organizations face. Determining an effective site provisioning and clean up approach that balances end-user control with effective information management for the organization is essential. This session shows developers how to create a flexible solution that lets users get sites up and running quickly, while maintaining stewardship for corporate resource concerns by providing site creation approval, site archiving and site removal strategies. In this session you'll see how to leverage Microsoft InfoPath as a site request form coupled with a SharePoint workflow to approve and create a site. You'll also see the use of new site-level workflows and auditing to monitor the use of the site and recommend when it's time to archive or delete it based upon usage.

HITP11: PROTECTING YOUR SHAREPOINT ENVIRONMENT FROM THE EVIL DEVELOPERS–QUOTAS, SANDBOXES, AND QUERIES
ROBERT L. BOGUE

Whether you believe your developers are evil or just under informed, SharePoint 2010 has a set of tools for you to use to protect yourself from a developer breaking your entire farm. In this session you'll get an IT Pro's introduction to the SharePoint Sandbox and how it can help you including code isolation and execution quotas. You'll also learn about protection from long running queries, and how you can put the pieces together to keep your farm running no matter what the developers throw at it.

HITP12: SHAREPOINT SOLUTION CREATION TOOLS FOR THE IT PRO WITHOUT SEMICOLONS
ROBERT L. BOGUE

Many organizations are struggling to get the support they need. The IT Pro is being asked to help create solutions for business units. The Office System including SharePoint, Visio, InfoPath, Word, and SharePoint Designer are tools that the IT Professional can use to create solutions that don't require a single semicolon. In this very practical session, we'll create a few solutions that every IT Pro can create that will look like you stayed up all night to learn a new (foreign) language.

HITP13: BEGINNING YOUR ADMINISTRATIVE JOURNEY WITH SHAREPOINT 2010
SHANE YOUNG & TODD KLINDT

Time to start talking install and deployment. What are these new things like Prereq installer, farm passphrase, managed accounts, Farm configuration wizard, and pretty icons in central admin? If these are your questions we have your answers. Even if they aren't your questions, swing by. We promise you'll learn something, or at least hear a bad cow joke or two.

HITP14: CONTINUING YOUR ADMINISTRATIVE JOURNEY WITH SHAREPOINT 2010

SHANE YOUNG & TODD KLINDT

Now your farm is running like a well-oiled machine time to look at the new tools. Things like PowerShell, monitoring, backup and restore, performance and large list throttling, and a few other fun things. So many new admin tools and so little time.

HITP15: ADMINISTRATION OF SHAREPOINT 2010 USING POWERSHELL, THE NEW COOLNESS

SHANE YOUNG & TODD KLINDT

All your friends are doing it why aren't you? Stsadm.exe is so 2007. Come to this session to figure out why you need to be a PowerShell guru ASAP and how to amaze your friends and confound your enemies with your new PowerShell skills.

HITP16: SHAREPOINT 2010 ADMINS AND THE DBA DUTIES THEY HATE

SHANE YOUNG & TODD KLINDT

Nobody likes it but it is a fact of life–SharePoint stores everything in SQL Server. Do you know where the most common performance bottleneck for SharePoint is? Your SQL Server. Yikes! So with that being the case, any good SharePoint Admin needs to be up to speed on core SQL Server management. In this session we'll demystify how SharePoint uses SQL, and show what maintenance steps you can take to keep SQL from taking its ball and going home.

HITP17: BETTER TOGETHER: SHAREPOINT, EXCEL, AND ACCESS DELIVER "BIG WIN" SOLUTIONS AND ADOPTION

DAN HOLME

In every organization, mission-critical business intelligence and processes center around Excel worksheets, Access databases, and e-mail-based communications. In this "Better Together" session, you'll learn how to elevate these using out-of-the-box functionality in combinations that achieve "big wins" and drive the success and adoption of SharePoint and Office in your enterprise. This session presents practical, real-world examples to inspire you to identify and solve business problems with SharePoint, Excel, and Access. Decision makers and even power-users will come away armed with an understanding of what amazing things SharePoint and Office can do, together, to deliver high-value solutions, and IT Pros will learn how to guide, implement, configure, and support such solutions. You'll discover approaches for integrating SharePoint, Excel, Access, workflows, Office Web Applications, and more. You'll also learn which solutions can be attained with previous versions of Office and with only SharePoint Foundation/Windows SharePoint Services, and which require SharePoint Server and Office 2010. Technical takeaways include:

- Move important, shared, or multi-user databases from their 20th century home in Excel worksheets and Access databases to SharePoint.
- Create rich, code-free "business intelligence lite" SharePoint solutions that apply SharePoint security and collaboration in unique ways and leverage Excel as an analysis and presentation tool.
- Develop sophisticated, intelligent relational database applications with gorgeous forms and reports using Access as a SharePoint front-end.
- Leverage the new and improved Excel Services and Access Services for high-value, low-effort database solutions.

ALSO:

GENERATE AND PUBLISH ELECTRONIC FORMS ON YOUR INTRANET USING INFOPATH 2010... NO CODE REQUIRED

ASIF REHMANI

Finally, you can make your goals of going paperless a reality! Microsoft Office InfoPath 2010 and Forms Server 2010 come together to provide a powerful platform for electronic form generation. In this session, you will see how you can build robust electronic forms with data validation and conditional logic rules using InfoPath. Also, the inherent power of InfoPath will be demonstrated to look up data from various sources and populate it in your custom designed electronic forms. All this and more will be accomplished without writing a single line of code!

SHAREPOINT DESIGNER 2010: TOP 5 GREAT THINGS TO KNOW!

ASIF REHMANI

SharePoint Designer 2010, which is a free application, is "The Preferred" tool to design powerful no-code solutions and applications in SharePoint 2010. In this session, you will get a broad overview of the capabilities of the tool, from site customizations such as modifying Site Metadata, managing Site Security, or creating Site Content, to building List- or Site-based Workflows and connecting to a variety of data sources. You will also learn about the new ribbon interface of SharePoint Designer 2010 and you'll see how best to take advantage of this application by showing the new bells and whistles that come with this product.

MARCH 16, 2009 9AM - 4PM

PRECON WORKSHOP (IT PRO): SHAREPOINT JUMP START: REIMAGINING COLLABORATION

DAN HOLME

If you are new to SharePoint, or are trying to wrap your head around the massive potential of this powerful platform, you'll be the hero of your enterprise when you bring back the solutions you discover in this fast-paced, full-day pre-conference workshop. Dan Holme, a Microsoft MVP for SharePoint, will dive deep into the configuration, customization, and management of SharePoint collaboration. You'll learn to build SharePoint solutions that address common enterprise challenges, and you'll be amazed just how much you can do with Windows SharePoint Services (WSS) without having to pay for Microsoft Office SharePoint Server (MOSS). Topics include:

- SharePoint Administration Jump-Start: What you need to know to administer SharePoint effectively, in 90 minutes or less.
- How to use SharePoint document libraries as a replacement for traditional file shares.
- Driving effective collaboration and end-user adoption with Microsoft Office 2007 applications as SharePoint clients.
- How to build "Business Intelligence Lite", no-code, and low-code SharePoint solutions using Office 2007 and SharePoint Designer.

PRECON WORKSHOP (IT PRO): SHAREPOINT SERVER 2010: FARM UPGRADE AND WHAT'S NEW FOR EXPERIENCED SHAREPOINT ADMINS

SHANE YOUNG & TODD KLINDT

So you are already an awesome SharePoint v3 administrator and you want to start on the road to awesome for SharePoint 2010. Well then come on down. This workshop will start your road to SharePoint 2010 cool with a bang. In this workshop, we will cover everything you need to know to get your 2010 farm up and running. From there we will work through all of the new functionality that makes being an administrator so much furn. And if that wasn't enough fun, from there we will explore upgrade. We figure since you have a perfectly running farm now we might as well look at the upgrade story for your 2007 content. It'll knock your socks off.

PRECON WORKSHOP (DEVELOPER): BUILDING COMPOSITE APPLICATIONS USING SHAREPOINT DESIGNER 2010 AND THE BCS

RAYMOND MITCHELL

In this full-day workshop, you'll learn how to use the new functionality available in SharePoint Designer 2010 to build advanced Composite Applications. Some of the topics covered include:

- How to leverage the Data Form Web Part and the new XLV to display and interact with your SharePoint Data. We'll also take a long look at the magic behind these Web Parts—XSLT.
- How to use the updated Business Connectivity Services to surface your business data. We'll also explore other options to incorporate external data into your Composite Applications.
- How to create powerful Workflows and add Custom Actions to transform your Data Views and Dashboards into interactive Applications.
- How to customize the look and feel of your Composite Applications to create a rich user experience. We'll walk through several real-world scenarios and give you the tools you'll need to build your own applications on top of the SharePoint platform.

PRECON WORKSHOP (DEVELOPER): DEEP DIVE INTO SHAREPOINT 2010 WORKFLOWS

ROBERT L. BOGUE

The Office 2010 system includes a much better transition between user developed workflows and developer workflows. Learn how SharePoint Designer can be used to start your workflow development process, how InfoPath forms can be your forms solution for your workflows, and how Visio is a part of the workflow development process. Once we've developed a workflow with end-user tools, we'll take it into Visual Studio and enhance it with things that you can only do in Visual Studio. We'll end with a discussion of Site Workflows and how they can be used.

FEATURED SPEAKERS

TODD BAGINSKI
INTELLIGENT EFFECTS

ROBERT BOGUE
THOR PROJECTS

ANDREW CONNELL
CRITICAL PATH TRAINING, LLC

KIRK EVANS
MICROSOFT

STEVE FOX
MICROSOFT

SCOT HILLIER
SCOT HILLIER TECHNICAL SOLUTIONS, LLC

JOHN HOLLIDAY
JOHN HOLLIDAY & ASSOCIATES, INC.

DAN HOLME
INTELLIEM, INC.

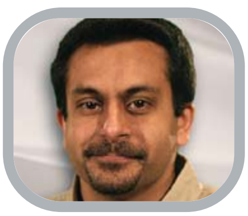
TODD KLINDT,
SHAREPOINT911

MATTHEW MCDERMOTT
CATAPULT SYSTEMS

RAYMOND MITCHELL
INETIUM

MICHAEL NOEL
CONVERGENT COMPUTING

TED PATTISON
CRITICAL PATH TRAINING, LLC



ASIF REHMANI
SHAREPOINT ELEARNING.COM

THOMAS RIZZO
MICROSOFT

SHANE YOUNG
SHAREPOINT911

And many more... *Check our Web site as we continue to update it with speaker pictures and bios!*

Hotel and Travel

Bellagio Resort & Casino, Las Vegas, NV

Grant yourself the luxury of discovery time as you explore the dramatic features which distinguish this exquisite Las Vegas resort from every other destination in the world. From dancing fountains to a breathtaking conservatory & botanical gardens to serenity-splashed pools & courtyards, plus a refreshing addition to your entertainment options, the world famous Fountains of Bellagio were destined to romance your senses. Take in a complimentary Las Vegas show of water, music and light thoughtfully interwoven to mesmerize its admirers.

HOTEL ACCOMMODATIONS BELLAGIO RESORT & CASINO

3600 Las Vegas Boulevard South, Las Vegas, NV 89119

Bellagio Resort & Casino is the conference site and host hotel. This is where all sessions and activities are held.

We have secured a discount conference rate of $149 per night plus tax (12%). Based on Availability. Rate is based on single or double occupancy. Hotel requires a one night room and tax deposit at time of reservation. (Credit card will be charged by the hotel). Hotel cancellation policy: Must cancel at least 48 hours prior to arrival date.

Space is limited so reserve your room early by registering online or by calling the conference hotline at 800-438-6720 or 203-400-6121. All reservations must be guaranteed with a major credit card to confirm room. A deposit of the first night room and tax will be charged. Cancellations must be received by the hotel 48 hours prior to the confirmed arrival date to receive refund of deposit

AIRLINE

Please call Pericas Travel at 203-562-6668 for airline reservations.

CAR RENTAL

Hertz is offering auto rental discounts to attendees. See the conference Web site for details.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information, contact Jackie Baillie
949-226-2313 phone • E-mail Jacquelyn.baillie@penton.com
See Web site for more details. www.sharepointprosummit.com

TAX DEDUCTION

Your attendance to this conference may be tax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

1-3 registrants	$1,395 per person
Additional registrants after the 3rd (4th, 5th, 6th...)	$1,195 per person ($200 off each)

Call 800-438-6720 to take advantage of group discount pricing.

Notes & Policies: The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.sharepointprosummit.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague by notifying us before the start of the event. Please inform us if you have any special needs or dietary restrictions when you register.

Registration & Cancellation Policy: Payment must be received before the start of the conference. Cancellations by February 15th, 2010 must be received in writing and will be refunded minus a $100 processing fee. After February 15th, 2010 cancellations and no-shows are liable for full registration fee, however registration can be transferred to the next Connections Conference within 12 months or to another person.

CONFERENCE REGISTRATION • MARCH 16-19, 2010

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON MARCH 17TH,
THROUGH CLOSING SESSION MARCH 19TH, 4:30PM

NAME ______________________ PRIORITY CODE ______________________

COMPANY ______________________ TITLE ______________________

STREET ADDRESS (REQUIRED TO SHIP MATERIALS) ______________________

CITY, STATE, POSTAL CODE ______________________ COUNTRY ______________________

TELEPHONE ______________________ FAX ______________________ E-MAIL ADDRESS (IMPORTANT) ______________________

ONLINE: www.SharePointProSummit.com
E-MAIL: info@DevConnections.com
PHONE: (800) 438-6720
(203) 400-6121
FAX: (913) 514-9362
MAIL:
SharePointPro Summit & Expo 2010
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

☐ **SharePointPro Summit & Expo** ***before*** JANUARY 15, 2010 .... $1195 ____________
after JANUARY 15, 2010 .... $1395 ____________

PRE-CONFERENCE WORKSHOPS TUESDAY, MARCH 16, 2010 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS ONLY.

☐ SharePoint Jump Start: Reimagining Collaboration HOLME .... 9AM - 4PM .... $399 ____________
☐ SharePoint Server 2010: Farm Upgrade and What's New YOUNG & TODD KLINDT .... 9AM - 4PM .... $399 ____________
☐ Building Composite Applications Using SharePoint Designer 2010 and the BCS MITCHELL .... 9AM - 4PM .... $399 ____________
☐ Deep Dive into SharePoint 2010 Workflows BOGUE .... 9AM - 4PM .... $399 ____________

CONFERENCE MATERIALS

FULL CONFERENCE REGISTRATION INCLUDES MATERIALS FOR THE CONFERENCE FOR WHICH YOU REGISTER;
YOU MAY PURCHASE MATERIALS FOR THE OTHER CONCURRENTLY RUN EVENTS.

☐ SharePointPro CD .... $75 ____________
☐ VirtualizationPro CD .... $75 ____________

TOTAL

☐ CHECK (payable to Tech Conferences) All payments must be in US Currency. Checks must be drawn on a US bank.
**IMPORTANT: Must reference which Connections conference you are registering for on your check.*

☐ CREDIT CARD ☐ VISA ☐ MASTERCARD ☐ AMEX

CREDIT CARD NO. ______________________ EXPIRATION DATE ____________

Cardholder's Signature ______________________ Cardholder's Name (print) ______________________

Penton Media

c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

Simplify EFS Deployment

Learn how to get the most out of EFS Assistant and EFS Certificate Updater

by Russell Smith

Microsoft's Encrypting File System (EFS), introduced in Windows 2000 Server, has improved over the years but still has limited out-of-the-box support for central management and control via Group Policy. The introduction of BitLocker Drive Encryption in Windows Vista and Windows Server 2008 changed the encryption ballgame somewhat, placing EFS in second place, because full disk encryption is acknowledged as the best method for securing data on notebooks. EFS works at the file level and offers some degree of manageability but it can't encrypt critical OS files. BitLocker works at a low level and encrypts entire volumes. Unlike EFS, BitLocker protects files in the Windows directory and OS files that may contain sensitive information.

Although EFS may still be useful in certain scenarios (e.g., protecting files where users have shared access), BitLocker is the primary choice for encryption on newer systems. But for those of us who need to provide a solution for encrypting sensitive data on Windows XP-based systems, without the expense of third-party solutions, EFS is still the first point of call.

Hidden away in the depths of Microsoft's Data Encryption Toolkit for Mobile PCs are two tools that can help you gain more control over EFS. The EFS Assistant can enforce encryption of files and folders and scan for files that should be encrypted, helping organizations adhere to regulatory requirements and security policy. The EFS Certificate Updater can help organizations move users from self-signed certificates to V2 certificates provided by a Certification Authority (CA).

One of the main restrictions of EFS on XP is that there's no way to enforce encryption of folders. Encryption can be enabled or disabled for domain computers in Group Policy, and Recovery Agents can be configured, but that's about it—administrators or users must configure the encryption status for each folder.

Installing the EFS Assistant

You can deploy EFS Assistant to client devices to automate encryption of potentially sensitive data that might otherwise be left exposed in the case of a physical breach. EFS Assistant is a small executable that can be installed on every Windows device in an organization (the tool currently supports only XP and Vista). It runs in the context of the logged on user. The tool scans files and folders, enabling encryption based on policy defined in the registry. You can download the tool at www.microsoft.com/downloads/details.aspx?FamilyId=1A99576A-FE67-418F-88B1-81E2055FE977.

Evaluation settings, the reporting tool, administrative templates, and shortcuts are installed by default only when the EFS Assistant MSI file is run interactively. The Evaluation Settings install option writes

Table 1: Rules Written to the Registry

Function	Registry Value	Standard Setting
Folder encryption mode	FolderEncryptionMode	Encrypts specified folders and folders that contain file types listed in the *File types to encrypt* setting
Debugging mode	DebugEnabled	Enabled
Display status balloons	DisplayBalloons	Enabled
File types to encrypt	FileExtensionsToEncrypt	.ppt, .pptx, .doc, .docx, .xls, .xlsx

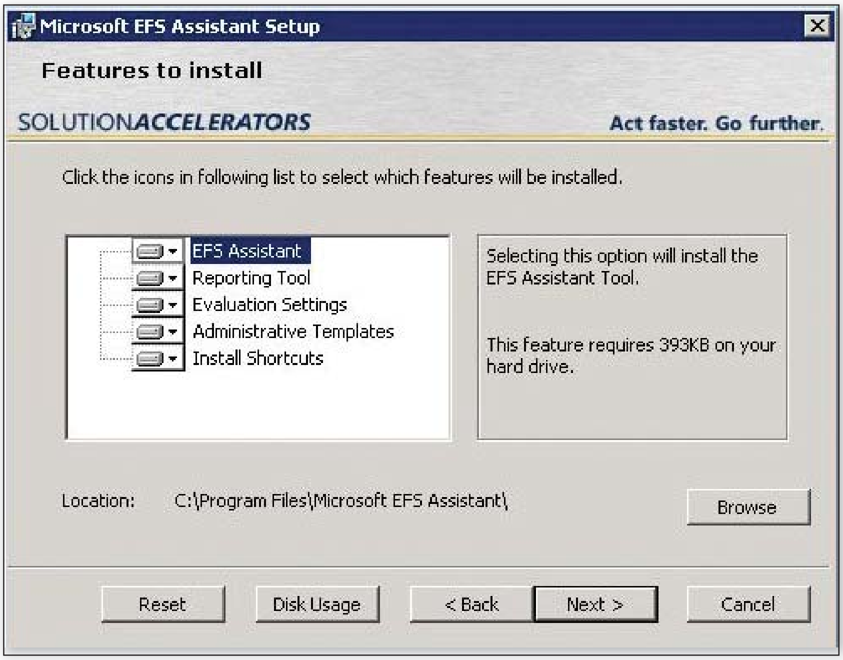


Figure 1: Microsoft EFS Assistant Setup

some basic rules to the HKLM\Software\Policies\Microsoft\EFS Assistant key in the registry on the local computer (Table 1).

To test the tool, run the EFS Assistant MSI file on an XP machine joined to your domain and accept all the default installation options (Figure 1). To start the tool manually, select All Programs, Microsoft EFS Assistant from the Start menu. Within a few seconds a balloon notification will inform you that the tool has started scanning files. In a domain environment, you can use Group Policy to deploy the tool and set it to run when users log on.

Another notification will appear once the scan is complete. Now you can run the reporting tool. Select All Programs, Microsoft EFS Assistant, EFS Assistant Results Viewer from the Start menu. This small Visual Basic script creates a CSV file (Figure 2) in the user's My Documents folder that contains details of encrypted files and folders from the computer's WMI database.

Configuring the EFS Assistant

When the tool is installed, two lists of folders are created: the Default Green and Default Red lists. These lists contain paths that the tool includes or excludes, respectively. Folders on the Default Green list include \%USERPROFILE%\Local Settings\Temporary Internet Files and \%USERPROFILE%\My Documents. Additional folder lists, which you can configure in Group Policy, take precedence over the Default Red and Green lists.

You can add EFS Assistant settings to Group Policy with the supplied Group Policy admin templates—EFSAssistant.adm and EFSAssistant.admx, for Windows Server 2003 and Server 2008, respectively. You'll find these templates in the Administrative Templates folder when you unzip the Microsoft EFS Assistant download. Log on to a domain controller (DC) as domain administrator, then

1. Open Group Policy Management Console (GPMC) and expand your forest

	A	B	C	D	E	F
1	Name	Classification	Source of Classification	Encryption Status	Encryption Substatus	Encryption Time
2	C:\Program Files\Common Files\Microsoft Shared\web server extensions\40\admcgi	Red	Inherited	Not Encrypted		
3	C:\Program Files\Solo9RusEngNum\IFaces	Red	Inherited	Not Encrypted		
4	C:\Program Files\VMware\VMware Tools\VAssert SDK\bin	Red	Inherited	Not Encrypted		
5	C:\Program Files\DivX\DivX Codec	Red	Inherited	Not Encrypted		
6	C:\Documents and Settings\user\Local Settings\Application Data\Google\Update\Manifest	Unclassified		Not Encrypted		
7	C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\User Data	Unclassified		Not Encrypted		
8	C:\Program Files\Common Files\System\msadc	Red	Inherited	Not Encrypted		
9	C:\Program Files\Common Files\Microsoft Shared\web server extensions\40\bin\1033	Red	Inherited	Not Encrypted		
10	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\YGKFY8MM	Green	Inherited	Encrypted	Encrypted This Run	17/02/200
11	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\6RWASJV1	Green	Inherited	Encrypted	Encrypted This Run	17/02/200
12	C:\Program Files\Internet Explorer\Connection Wizard	Red	Inherited	Not Encrypted		
13	C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\User Data\Default\	Unclassified		Not Encrypted		
14	C:\Program Files\Common Files\SpeechEngines\Microsoft\Lexicon\1033	Red	Inherited	Not Encrypted		
15	C:\Documents and Settings\user\Local Settings\Apps\2.0\Data	Unclassified		Not Encrypted		
16	C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.5\RedistList	Red	Inherited	Not Encrypted		
17	C:\Documents and Settings\user\My Documents	Green	Default Folders	Encrypted	Encrypted This Run	17/02/200
18	C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\1.0.154	Unclassified		Not Encrypted		
19	C:\Program Files\Common Files\Microsoft Shared\DW\1033	Red	Inherited	Not Encrypted		
20	C:\Documents and Settings\user\Local Settings\History\History.IE5	Green	Inherited	Encrypted	Encrypted This Run	17/02/200
21	C:\Program Files\Common Files\VMware\Drivers\Virtual Printer\TPOG3	Red	Inherited	Not Encrypted		
22	C:\Program Files\MSN Gaming Zone	Red	Inherited	Not Encrypted		
23	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\index.dat	Green	Parent Folder Encrypted	Not Encrypted	Access Denied	
24	C:\Program Files\xerox\nwwia	Red	Inherited	Not Encrypted		
25	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\W2P5KRU6	Green	Inherited	Encrypted	Encrypted This Run	17/02/200
26	C:\Documents and Settings\user\Application Data\Identities\{56DC0C1D-4E9F-40A3-AF6A-FCB58A3B7	Red	Inherited	Not Encrypted		
27	C:\	Unclassified		Not Encrypted		

Figure 2: CSV file detailing encrypted files and folders

and domain in the left pane.

2. Right-click the Group Policy Objects folder and select New from the menu. In the New GPO dialog box, enter EFSAssistant in the Name field and click OK.

3. Expand the Group Policy Objects folder, right-click the new EFSAssistant GPO, and select Edit from the menu. The Group Policy Management Editor window will open.

4. Expand Computer Configuration in the left pane of the GPO Editor, and right-click Administrative Templates. Select Add/Remove Templates from the menu.

5. Click Add at the bottom of the Add/Remove Templates dialog box and browse to the EFSAssistant.adm file in the Administrative Templates folder; click Open.

6. You should now see EFS Assistant appear under Current Policy Templates in the Add/Remove Templates dialog box. Click Close.

7. Expand Administrative Templates in the GPO Editor and select EFS Assistant (Figure 3).

As you'll see in the GPO Editor (Figure 3), management settings (most of which are self-explanatory) are expanded considerably with use of the EFS Assistant. In a production environment, you should make sure that you use Group Policy Scope of Management to deploy the tool and settings only to systems that meet the tool's system requirements. The EFS Assistant MSI installer file supports the /quiet switch on the command

Figure 3: Group Policy Object Editor

line for Group Policy Software Installation. When the /quiet switch is used, only the EFS Assistant executable is installed and no user interaction is required to complete the install process.

You can find best practices for deploying EFS at support.microsoft.com/kb/223316. You can find more information about the tool, including details about folders that should not be encrypted, in the Administrator's Guide supplied with the tool download.

Migrating to V2 Certificates with the EFS Certificate Updater Tool

So far, assuming there's no CA installed in your domain, files have been encrypted using self-signed certificates. Despite being a valid way to implement EFS, files encrypted with self-signed certificates cannot easily be shared with other users. And if a user's certificate is lost or corrupted, files must be recovered by a Data Recovery Agent (DRA).

The principle advantage of using V2 certificates is that they support key archival, so administrators can quickly give users access to encrypted files if their certificates are lost or corrupted. V2 certificates are supported in Enterprise and Data Center editions of Server 2003 (and later). If an appropriate V2 certificate has been installed in a user's personal certificate store, the EFS Certificate Updater tool changes the user's EFS configuration from a self-signed or V1 certificate to the V2 certificate. In an ideal situation, EFS should be disabled until all users have an appropriate V2 certificate for

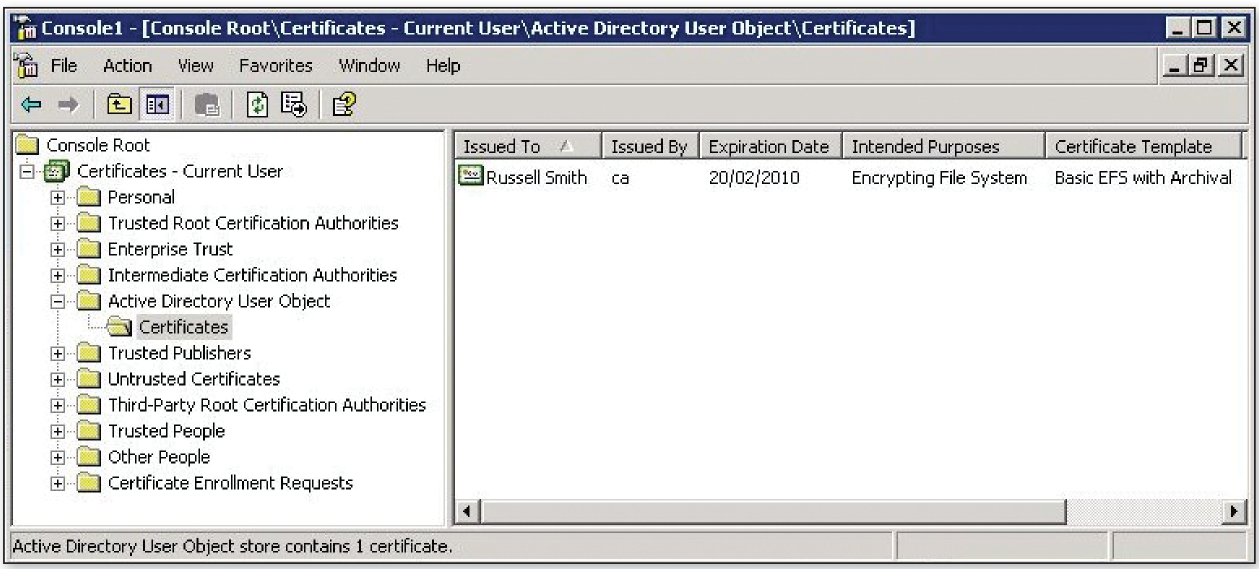


Figure 4: Determining whether users have an EFS V2 certificate

encrypting files in their personal certificate store. However, there may be situations where users have already encrypted files with a V1 or self-signed certificate. Even if those users successfully request a V2 certificate, EFS will continue to use the old certificate to encrypt new files. Previously encrypted files will remain encrypted using the old certificate.

To migrate to V2 certificates for users who have already encrypted files using a self-signed certificate, log on to XP with the user's account. Note that users must already have an EFS V2 certificate (Figure 4, page 51) in their personal certificate store before running the EFS Certificate Configuration Updater. The following commands could also be included in a logon script to automate the migration process across multiple computers. You can download the EFS Certificate Configuration Updater at www.codeplex.com/EFSCertUpdater/Release/ProjectReleases.aspx?ReleaseId=19752, then

1. Run the EFS Certificate Configuration Updater either from the command line or by double-clicking the executable. If you want to migrate from V1 certificates, you'll need to include the /m1 switch.
2. Open a command prompt and run cipher /u to update all previously encrypted files to use the new V2 certificate.
3. Log off and on again to ensure that Windows Explorer displays the correct thumbprint for encrypted files.

To check the results, compare the certificate's thumbprint on existing and newly encrypted files against the thumbprint of the V2 certificate in the user's personal certificate store.

1. Right-click an encrypted file that existed before you ran the EFS Certificate Configuration Updater.
2. In the file's Properties dialog box, click Advanced in the Attributes section.
3. In the Advanced Attributes dialog box, click Details under *Compress or Encrypt attributes*.
4. The Encryption Details dialog box will display the thumbprint of the certificate used to encrypt the file (Figure 5).
5. Type *mmc* in the Run box on the Start menu.
6. Click CTRL+M in the MMC window and then Add on the Add/Remove Snap-in dialog box.
7. Double click Certificates in the Add Standalone Snap-in dialog box.
8. Select *My user account* in the *Certificates snap-in* window and click Finish.
9. Click Close and then OK to return to the MMC window.
10. Expand Certificates – Current User, Personal, Certificates in the left pane and locate the V2 certificate issued by your CA in the right pane.
11. Double-click the certificate and select the Details tab in the Certificate dialog box.
12. Scroll down to the bottom of the list to view the certificate's thumbprint (Figure 6).
13. Compare the thumbprints from step 4 and step 12; they should be the same if cipher.exe successfully updated the certificates on encrypted files.
14. Repeat steps 1 through 4 to check that new files are also encrypted with the V2 certificate.

Figure 5: Encryption Details dialog box

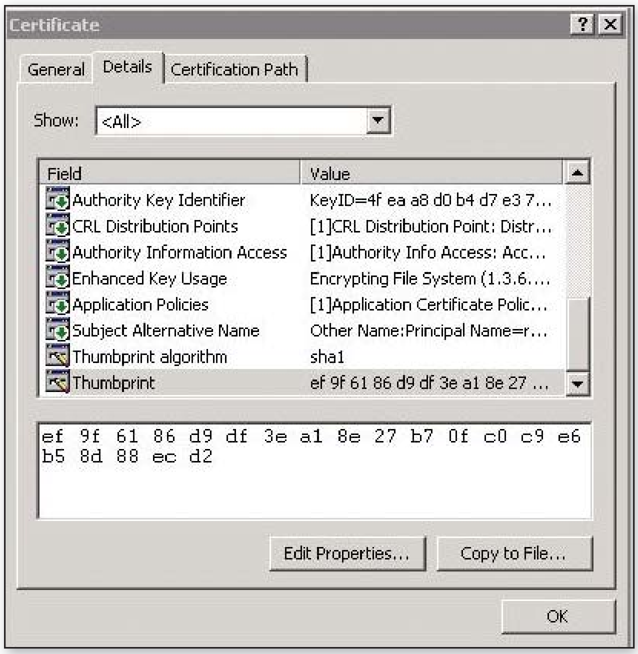


Figure 6: Viewing a certificate's thumbprint

EFS Gains Manageability

The EFS Assistant, while not foolproof, helps establish central management for encrypted files across your mobile workforce. Although Microsoft doesn't support the EFS Assistant on standalone computers, in my tests I found that it works as expected. In conjunction with cipher.exe, the EFS Certificate Configuration Updater provides quick and painless migration from self-signed or V1 certificates, directly to more flexible V2 certificates.

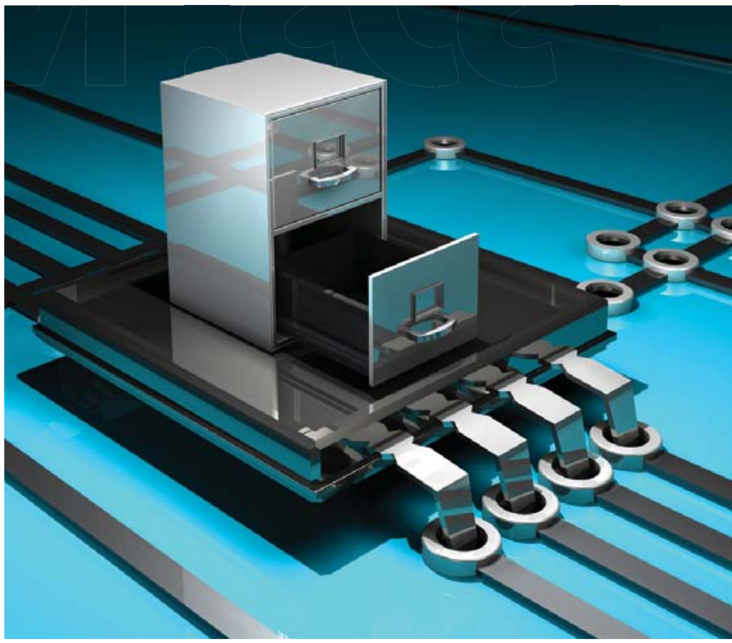
InstantDoc ID 102996

Russell Smith
(ms45@rsitc.com) is an independent IT consultant. He has been working in IT since 2000, specializing in systems management and security.

Exchange Storage: DAS vs. SAN vs. iSCSI

Making the right choice for your Exchange Server deployments

by Lee Dumas



Choosing the right storage system is critical for a successful Exchange Server 2007 deployment. Exchange Server supports three primary types of storage technologies: DAS, SAN, and the iSCSI protocol. There are advantages and disadvantages to each of these storage management options, but all three options are based on simple spinning disks.

Microsoft offers several tools that can help you determine your storage needs, such as the Exchange Storage Calculator and Jetstress (both available on Microsoft's site) to help you quantify your needs. Other free tools are also available, such as Iometer (www.iometer.org). Properly identifying how you'll use your storage before you commit to an option can save you time and money.

DAS has been around for decades and is a common choice for Exchange Server storage in small-to-midsized businesses (SMBs), and is increasingly common in enterprises as well. When considering DAS for your Exchange environment, you should investigate the various RAID array options and the importance of multiple disks.

SANs are dependable and scalable centralized data storage resources. SANs operate on their own independent networks and generally use connections based on Fibre Channel (FC) to communicate between various disks and connected hosts. Their drawback is that they're more expensive and more complicated than other options. Software for SANs tends to cost more than that for DAS arrays and is usually packaged separately from the hardware, whereas DAS arrays often include a set of utilities.

iSCSI is a storage protocol used to connect to a network device that moves storage-related data. It allows clients to send SCSI commands to remote, consolidated storage targets (or disk arrays) in the same way the client can interact with a locally attached disk. A common misconception is that you can connect iSCSI over your existing LAN infrastructure. Although this is technically possible, it isn't recommended. iSCSI devices are less expensive than FC devices, but you should still use dedicated hardware and cables. At the very least, you should have a dedicated virtual LAN and keep your devices relatively close together—running iSCSI over a WAN isn't a good idea.

NAS vs. iSCSI

iSCSI is sometimes incorrectly referred to as NAS. Although iSCSI storage systems are connected to a TCP/IP network like NAS, iSCSI isn't the same as traditional NAS. NAS is a type of device rather than a protocol. NAS uses standard network protocols, such as Server Message Block (SMB) and the Microsoft Windows Network, to emulate a storage device. iSCSI is a true storage protocol that is supported for Exchange deployments.

Traditional NAS is no longer supported in Exchange 2007, as stated in the Exchange team's blog at tinyurl.com/2pendn. Even in Exchange Server 2003 installations, Microsoft supports only the use of Microsoft Windows Hardware Quality Labs qualified NAS storage devices. I haven't had good experiences with any NAS products; if you're determined to choose NAS, check with your vendor to ensure the end-to-end solution is designed for use with Exchange 2003.

The most important consideration when selecting an Exchange Server storage configuration is to make sure it will fit your business needs. Each option has its benefits and drawbacks.

DAS: Cheap and Easy

There's a good reason DAS is so common for Exchange Server storage—it's the cheapest and best performing of the three approaches presented here. DAS uses one host and is best for SMBs, but it poses significant challenges when scaling to many users. If you need to add spindles for extra space and performance, DAS solutions might not expand as easily as SAN solutions.

How the DAS solution will be managed long term should be another key part of your decision process. Keep in mind that there are several factors involved in calculating the cost of storage, and capital expenditure is just one—DAS might seem cheap up front, but remember to take into account the cost of managing it long term.

In a DAS environment, more spindles equals higher I/O operations per second (IOPS) capacity and better IOPS performance. The size of the individual disks affects data storage, but your I/O rate will be significantly better with a RAID array of ten 180GB drives than with an array of six 300GB drives. Capacity and I/O throughput don't increase at the same rate.

Using a RAID array with fault tolerance can increase your financial overhead costs and decrease performance, but you can add additional disks to an array to speed up your I/O on top of the added tolerance. Using such an array is well worth the investment if you want to avoid permanent data loss and potential downtime to the end user.

SAN: Costly, Complex, and Extremely Capable

SANs are the best centralized data storage option if cost and complexity aren't issues for you. SANs have high data throughput and excellent fault tolerance—not only are the disk arrays fault tolerant, the connections themselves are fault tolerant as well. Multiple data paths ensure that there's always a route to the required storage. SANs are also very scalable—they can have multiple hosts and you can add new volumes or expand existing storage as you need it.

SANs have traditionally been used with FC connections, but FC is usually a problem for smaller businesses because it's expensive and requires complex configuration. In my experience, there are very few well-trained engineers. Employing these engineers full time to help with your storage infrastructure can be costly, and the learning curve for deployment and maintenance is massive. SAN vendors usually have services to assist in configuration and initial setup, but these services can be costly, especially if you have a changing environment.

Unfortunately, there aren't any comprehensive, cross-platform tools that will manage all brands of SAN devices, so to minimize the probability of complications, it's best to stick with a specific product set and a single vendor. This will make life easier on you and your Exchange team, because each SAN vendor implements slightly different configurations for creating and presenting storage to hosts. Plus, the SAN itself will likely have to deal with various servers running different OSs.

Many companies use a SAN for applications other than Exchange, such as SQL Server or SharePoint, in addition to Exchange. Using a SAN for multiple applications can reduce the cost of SAN storage for Exchange by spreading the costs around, but in my experience, most Exchange deployments should use disks that are separate from those used by other applications. I've seen plenty of customers try "sharing spindles" only to find that their SANs couldn't handle Exchange's I/O plus the other I/O on the same set of disks.

SAN with iSCSI: An Alternative to FC

iSCSI SANs are a less expensive alternative to FC, and they work for both large and small companies. iSCSI SANs are configured from the host or device itself, so they're simple to configure, too. iSCSI SANs are comparable to FC with regard to data transport security, because connections can be authenticated or encrypted as long as both the initiator and target systems support the required protocols. The drawback is that iSCSI isn't always as fast as FC, but despite this, iSCSI's versatility and lower price tag are making it more popular.

You'll probably want to use a hardware-based iSCSI or TCP/IP Offload Engine (TOE) adapter to optimize performance. Using a TOE iSCSI adapter lets much of the communication process be handled by the processer and memory in the adapter itself, unlike software-only iSCSI solutions, which can get bogged down in heavy load environments.

RAID Levels

RAID is an all-encompassing term for data storage schemes that divide and duplicate data across multiple disk drives. The data is spread across the array of disks, but users and the OS see the array as one entity.

When selecting and designing a RAID solution for your Exchange server, keep in mind the amount of disk space you'll need and the amount of rebuild time your company can withstand if something happens to your array. A RAID array with larger disks will take longer to rebuild than one with smaller disks, and one with Serial ATA (SATA) disks will take longer to rebuild than one with Serial Attached SCSI (SAS) disks. Adding more disks to the array will increase build times as well. There are several levels of RAID that can be used for Exchange Server.

Exchange 2010 Considerations

Disk Type

Exchange Server 2010 has major improvements in the way it utilizes the storage system. In Exchange Server 2007, it was common for customers to use high-speed FC or SAS disks because of their IOPS capacity. Exchange 2010 has a significantly lower IOPS profile than previous versions, so you might not require FC or SAS disks for performance any longer.

RAID Types

Databases Availability Group (DAG), a new feature in Exchange 2010, allows for configurations that don't require RAID on the server. A configuration known as Just a Bunch Of Disks (JBOD) has been added to provide for additional customer choice. JBOD is accomplished by application-level database replication as part of DAG's functionality.

IOPS / Memory Calculation

More than ever, it's important when using Exchange 2010 to take the time to estimate the correct amount of memory and IOPS load/capacity needed for deployments. Exchange 2010 has much higher memory requirements for large mailbox support than past versions, and all Exchange 2010 designs should use the Microsoft best practice guidelines and test tools for final validation.

Third-Party Impact

As more and more applications take advantage of Exchange, it's common to see Exchange deployments that are undersized because third-party use hasn't been factored into their designs. When designing an Exchange 2010 system, ensure that all third-party applications are accounted for. Wireless devices, third-party add-ins for Outlook, and others all have an effect on the overall performance of your Exchange server.

RAID 0 arrays split and distribute, or "stripe," data across several disks. In a RAID 0 array, you can use the full storage capacity of all of your disks—two 300GB drives will give you a total storage capacity of 600GB. RAID 0 arrays offer good performance because they can write simultaneously to each drive, but their drawback is that they don't offer fault tolerance. If one disk in a RAID 0 array fails, the entire array is destroyed and you'll lose all data on all disks. Because of this risk, RAID 0 isn't recommended for use in any business-critical capacity.

RAID 1 is a mirrored, or duplicated, set of disks. RAID 1 setups are composed of an even number of disks, and all data written to one drive is also written to another, so if one disk fails, you won't lose any data. RAID 1 is a good choice for OS partitions and Exchange database logs, and is the most common RAID level used for transaction logs. A drawback of RAID 1 is that while some RAID 1 configurations allow simultaneous reading from two disks at once for improved read times, mirrored arrays are no faster at writing than using a single disk. Also, in RAID 1 configurations you can only use half the capacity of your disks, because all data is written twice.

RAID 0+1, as the name implies, is a combination of both RAID 0 and RAID 1 arrays, where data is both striped and mirrored to provide fault tolerance and performance improvements. RAID 0+1 setups are fairly expensive because of the duplicate disks (they require at least four disks—two striped disks and their mirrored duplicates), but the improved fault tolerance and increased speed is usually worth the additional cost and complexity. RAID 0+1 is the most common RAID level for Exchange databases.

RAID 5 is another fairly common option for use in Exchange Server 2007. RAID 5 is a set of striped disks that relies on parity to protect you from data loss. Data is spread across all the disks in a RAID 5 array, and if one disk fails no data is lost, but no disk is a duplicate of another in the array. The performance of RAID 5 is about a third of that of RAID 1 and 0+1, because each write to the OS requires three writes to disk. The storage capacity of a RAID 5 array is reduced—the total capacity of a RAID 5 array is equal to the capacity of all the disks in the array minus the capacity of one of those disks. That reduced capacity combined with its slower performance may make another configuration preferable to RAID 5.

To determine which RAID level is best for your environment, you should assess what the impact of RAID will be on the overall IOPS capacity of your drive system. RAID 1 and 0+1 don't have any impact on the drives' ability to handle IOPS, but RAID 5 will produce only one third the performance of the same drives in a non-RAID 5 configuration. During the design phase, it's important to evaluate all of the RAID options or work with someone who can guide you through the complexities of storage architecture design. Be sure to take advantage of tools from storage vendors and the tools I mentioned in the introduction to test your storage systems and make sure they're meeting your requirements.

Configurations to Fit Your Business Needs

The most important consideration when selecting an Exchange Server storage configuration is to make sure it will fit your business needs. Each option has its benefits and drawbacks. For example, don't use an unsupported version of NAS. If you have a limited storage budget, don't opt for an FC SAN. Don't forget to test everything before putting your new disk system into a production environment. I recommend using Jetstress to make sure everything works before you take the leap and make your system live.

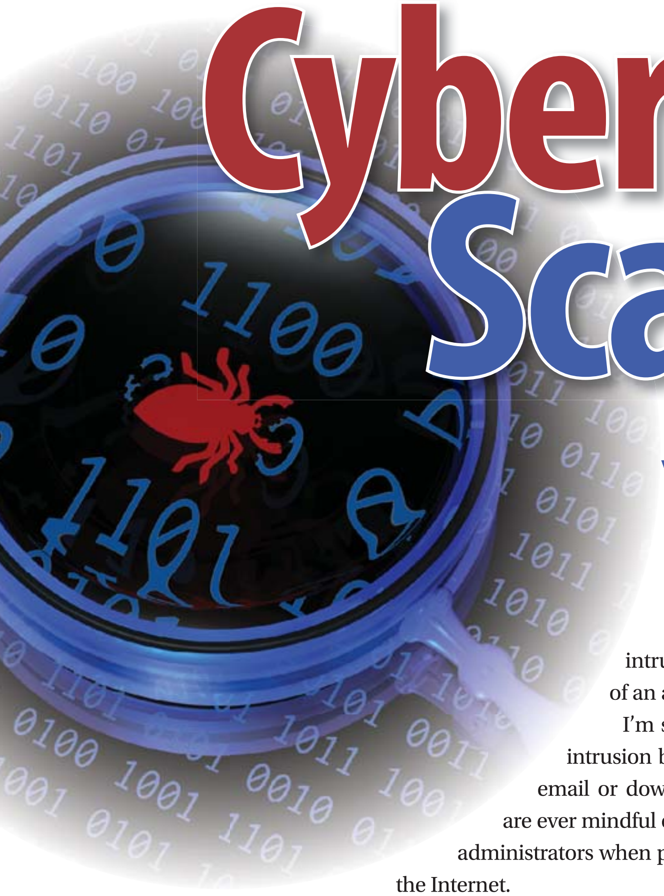
You're likely to find that one of the options discussed will provide a workable solution to fit the performance, scalability, and budget requirements of your environment, regardless of what version of Exchange you're running. I'd like to hear how you've managed to circumvent tricky environments to improve your Exchange storage infrastructure, so feel free to drop me an email.

InstantDoc ID 103013

Lee Dumas
(lee.dumas@azaleos.com) is director of architecture for Azaleos, a provider of remote management services for Exchange, and a Microsoft Certified Architect. He previously served on Microsoft's Exchange development team and has worked with Exchange and messaging for 15 years.

FEATURE

Cyber Threat Scanner



You never know when you'll be called upon to do an immediate scan of your systems for known intrusive files. Even with the best maintained and accurate antivirus applications running, there is always a possibility that something will get through. In general, antivirus updates are only as current as known viruses. Unfortunately, fixes are not available until shortly after a new intrusion has been discovered. So someone is bound to be the unwitting recipient of an attack or intrusion.

I'm sure that most of us have very secure systems and might have never had an intrusion beyond the occasional desktop virus triggered by a user opening an enticing email or downloading questionable files over the Internet. Of course we administrators are ever mindful of such events and help keep our systems safe by avoiding being logged on as administrators when performing non-administrative tasks such as opening our mail and accessing the Internet.

Home-grown utility eases the search for intrusive files

by Jim Turner

In any event, there is a vital need to have a system in place that can scan your computer systems at a moment's notice for intrusive files that might have entered your systems via virus attack, worms, hackers, malware, or other means. In many businesses nowadays, there is also the need to comply with security initiatives that require IT administrators to scan for specific files on occasion even if they have not necessarily experienced problems. Aside from a very resource-intensive effort to have the IT staff frantically perform manual scans of all systems, there is not really much available with the major Windows systems that allows you to run these scans easily and effectively across an entire domain.

The Application

I created the Cyber Threat Scanner, which wraps two third-party utilities within VBScript. I made the choice to use these utilities instead of pure VBScript simply to overcome the lengthy processing time that would be involved if the application were written purely in VBScript.

The first utility is a freeware package from Mythicsoft called Agent Ransack, which is the search engine beneath the Cyber Threat Scanner application's hood that scans for the files you're looking for. You can download Agent Ransack at www.mythicsoft.com/agentransack/download.aspx. The second utility is a public domain utility called MD5deep, which can produce MD5 hashes of files and can perform hash comparisons of the files against a list of known intrusive file hashes. You can download MD5deep at md5deep.sourceforge.net.

To actually make this application function quickly and scan many systems at the same time, it was necessary to make it a multithreaded application. This is not a true multithreaded application by definition but rather a pseudo-multithreaded application that calls a secondary script multiple times. This secondary script performs the search against multiple servers—and because all the secondary scripts run simultaneously, it's loosely considered to be multithreaded.

This is an extremely sensitive and important process, and with that comes a good bit of preparation before running the main VBScript file. You must:

- Define regular expressions of the intrusive filenames
- Create a list of computers to be scanned
- Create a hash list file that lists the 32-character strings of the intrusive files

To make this preparation process more streamlined and less stressful, I also created an HTML Application (HTA) called CyberScanPrep.hta that ties these preparation requirements together. Figure 1 is a snapshot of what the prep application looks like, complete with the general Help screen that the application provides. Additionally, each input area offers detailed context-sensitive help about the specific entry. (You can download CyberScanPrep.hta at www.windowsitpro.com; enter 103078 in the InstantDoc ID text box and click Download the Code Here.)

Entering Information

In most cases, you'll be provided with filenames and associated MD5 hashes of the intrusive files by your security department or management. When hash strings of intrusive files are provided, you can precisely determine whether a file that has the same name as an intrusive file is actually an intrusive file or not, greatly reducing the amount of work you have to perform after the scan is done. I have, however, left the application open to the possibility that you might simply need to search for files without hashes, in which case you would simply check a check box within the prep application. However, this is not the norm; you should, in most cases if not all, receive hash strings with the request to search for particular cyber threat files.

The first input box in the prep application is designed to hold the 32-character hash strings and associated filenames. To avoid mistakes and to overstate the obvious, you should always copy and paste the strings from a document that you received from security or management. After pasting a hash string, add two blank spaces and enter the associated filename. If you have more than one hash string to enter, use a carriage return after each entry and then enter the next one. Continue to do this until you have entered all the hash strings.

Keep in mind that this application is limited to searching for a maximum of nine files (the maximum allowed by the free version of Agent Ransack). I personally have never had to search for more than just a few, but should you be confronted with a request to search for more than nine files, you should have another person set up this application on another machine and run the process to search for the additional files.

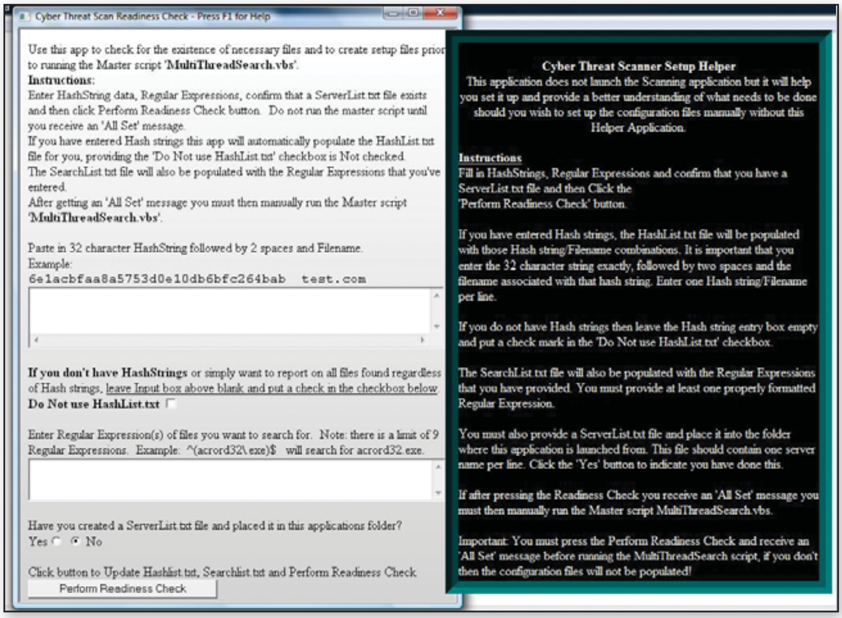


Figure 1: Cyber Threat Scanner Setup Helper

If for whatever reason you do not receive hash strings with the list of files to search for, make sure you put a check mark in the *Do not use HashList* check box. It's important to note that checking or clearing the check box determines whether the application performs a hash check against files found and the hash strings contained within the HashList.txt file. If a hash file is used, only files found that have matching hashes will be considered "Found" intrusive files.

Entering Regular Expressions

The second input box is for the list of files you want to search for. Agent Ransack allows for a great deal of flexibility when searching for files, letting you enter regular expressions of the files you're looking for. For those with experience with regular expressions, this should be pretty straightforward. Just enter a regular expression for each file you want to search for. Remember that you're limited to nine entries.

For those not experienced with entering regular expressions, take a look at the example that is just above the input box. You'll see that it starts with a caret character, followed by an open parenthesis, the filename, a forward slash, a period, the file extension, a closing parenthesis, and the dollar sign.

The main points to understand here are:

- The caret, which means "Begins with"
- The open and closing parentheses, which mean look for this phrase within the parentheses
- The backslash is an escape character; because the period that would separate the filename and extension holds significant functionality in regular expressions, the backslash simply means use the period literally, not as a regular expression identifier
- The dollar sign at the end means "Ends with"

For the most part you'll be asked to look for specific filenames, so you won't have to have an extensive knowledge of regular expressions. Simply follow the example of entering caret, open parenthesis, filename, backslash, period, file extension, close parenthesis, and dollar sign. If you do have to come up with a more complex regular expression, you can launch AgentRansack.exe and use the Expression Builder to establish the correct regular expression.

The next entry on the prep application requires that you create a server list. Then, click the radio button indicating that you have done so.

Finally, perform the readiness check. If you haven't completed the required preparation, you'll be alerted as to what you need to do. If you've completed the preparation, you'll receive an All Set notification. You can then run the main VBScript file (MultiThreadSearch.vbs), which Web Listing 1 (www.windowsitpro.com, InstantDoc ID 103078) shows. I don't run the scan directly from the prep application for two reasons. First, HTAs aren't well behaved when they run long processes; they are like blobs on the screen that you can't do anything with until the process completes. Second, I

prefer to do a last-minute spot check of key files before launching the MultiThread-Search script. The prep app takes care of creating the HashList.txt file that contains the hash strings and it also takes care of creating the SearchList.txt file that contains the regular expressions Agent Ransack will use.

The default multithread setting is 20, meaning it will scan up to 20 servers at a time. You can change this setting by editing MultiThreadSearch.vbs and adjusting the TotalThreads variable. Keep this number between 15 and 30.

The application is designed to use and create all the necessary files in one parent folder. Create an appropriate folder and copy all the downloadable files from this article into that folder. You must also download and copy AgentRansack.exe and MD5deep.exe into this same folder before running the MultiThreadSearch.vbs script.

The Process

The first phase of the process uses Agent Ransack to produce log files of files found on every drive of every server contained within the ServerList.txt file. It writes these log files to the RansackLogs folder. If one or more files is found on a server that matches the search criteria (regular expression) contained within the SearchList.txt file, the log file will have a size greater than zero. If no files are found, the log file will have a file size of zero.

The second phase steps through each of the Agent Ransack-produced log files (those with file size greater than zero), reads the filename within the text file and runs the MD5deep utility to produce a hash for the file found, compares that with the hash strings within the HashList.txt file, and writes the file size, hash string, and filename to a hash results log file in the HashLogs folder if a matching hash string is found.

After all the Agent Ransack log files have been read and all the hash results log files have been written, the final stage of the process reads all the hash results logs, compiles all the data found within the hash results logs, and produces the Results.txt file. This is the file you'll use to determine if any intrusive files were found. If files are found, the results text files will show the server and complete paths of the files in question.

When the process finishes it creates .sav files of all significant files. These are copies of major contributing setup files involved with the search. A copy of the following files will be made with a .sav extension:

- ServerList.txt
- SearchList.txt
- HashList.txt
- MD5batch.cmd
- ErrorFile.txt
- Results.txt

When the main process is run again to do a new search, the .sav files are moved to archive folders along with the major log files from the HashLogs folder and the Ransack Logs folder that were produced from the previous run, in effect producing archives of all your scans.

The archive folders are named with specific dates that coincide with the original run date. When you're considering how to construct your list of servers to scan, you can create your own ServerList.txt file or you can create a server list automatically by running another utility script I created called Create ServerList.vbs, which Web Listing 2 shows.

It's important to note that the ServerList .txt file produced by this script will:

1. Include cluster servers but not cluster resources
2. Include domain controllers (DCs)
3. Gather from hard-coded organizational units (OUs) (OU=xxx,OU=xxx,OU=xxx), so you'll need to edit the script and adjust it to the appropriate OU
4. Gather any Active Directory (AD) computer where *operatingSystem* contains *Server*

CreateServerList.vbs will also produce a file called NoPingResponseServers.txt, which will contain any servers that could not be pinged. These servers will not be included in the ServerList.txt file. The main process (MultiThreadSearch.vbs) will also produce an ErrorFile.txt file; if any servers cannot be accessed via the script, they will be written to this file.

If you'd rather not use the prep application, you'll need to pay particular attention to the MD5batch.cmd file and edit it appropriately before you begin the search. The cmd file includes clear comments on which line needs to be open and which line needs to be commented out. Basically, the command file can produce an output file containing the hash string of any file passed to it. However, the cmd file contains one command that will compare the hash of a given file with a list of given hashes contained within the HashList .txt file. The cmd file also contains another command that will not compare the hash with the HashList.txt file. You can use only one of these command lines; the other must be commented out.

If the MD5batch.cmd file is set to use the HashList.txt file, be sure to remove any previous hashes and enter the new hash or hashes into the HashList.txt file. Each hash line must start with the 32-character hash and be followed by two spaces and the filename that is associated with that hash.

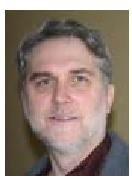
Note that if you specify that you want to use a HashList.txt file within the MD5deep .cmd file, the Results.txt file will contain only file information of files that have matching hash strings. In other words, even if you find a matching filename, if the hashes don't match, you won't see it reported in the Results.txt file. If you do not specify that you want to use the HashList.txt file, hash strings will appear in the Results.txt file for all files found matching the filename search criteria.

If you decide not to use the prep application, you'll also need to manually create the SearchList.txt file. This file will contain the list of filenames that you want to search for; they must be expressed in the form of regular expressions. Remember, there's a limitation of nine entries.

Depending on the machine you run the solution on and how many threads you want to spawn at one time, this application could be very resource and process intensive. You might want to set it up to run on a more powerful segregated computer. Also, be aware that the application could run for a very long time depending on how many servers you have, how many files were found, and the size of the files found.

I hope you won't have to use this application very often. However, if you do, I'm certain that it will help make the experience more tolerable and your day at work a whole lot less stressful.

InstantDoc ID 103078



Jim Turner
(jturnervbs@gmail.com) is a domain administrator and applications developer for Computer Sciences Corporation.

MOVING EXCHANGE TO THE CLOUD PART 1

Experience Exchange with low cost, high flexibility

by Tony Redmond

As evidenced in announcements and product introductions at events such as the Microsoft Professional Developers Conference (PDC) in 2008 and 2009 regarding Microsoft Azure, Microsoft Online Services, and new web-based versions of some Office applications, Microsoft has declared its strategic intent to be a major player in cloud-based computing. Chris Capossela, Microsoft senior vice president for Office, was widely quoted at the time, predicting that 50 percent of the Microsoft Exchange Server installed base will be online by 2013. Some of these mailboxes will come from the existing installed base and some will come through migrations from other email systems, such as Lotus Notes (see blogs.zdnet.com/microsoft/?p=1405).

The data includes mailboxes that Microsoft will migrate to Exchange between now and 2013, but it's still a lofty goal to transform half of an installed base from one computing model to another in four years. Commentators such as the Radicati Group predict that hosted email seats will grow by 40 percent by 2012 (bit.ly/3EFpgQ), largely driven by deployments within small and medium companies. They also predict that large enterprises will increasingly analyze the value that hosted email can deliver, especially for regional offices. Recent economic weaknesses will make CIOs consider how to cut costs wherever they can.

The ability to move to a fixed-cost offering is attractive, especially when Microsoft and Google are competing to reduce prices. Microsoft announced a reduction to $10 per user, per month for Business Productivity Online Standard Suite in November 2009. This price point gets close to Google's pricing for Google Apps Premier Edition while offering a familiar and more functional offering. All in all, it's a good time to be a purchaser of email services.

As Microsoft prepares for the deployment of Exchange Server 2010 as the basis of its managed email service, it's likely that the company will encourage customers to assess Microsoft Online Services as an upgrade option. In reviewing the options that will exist for customers in the 2009 to 2012 timeframe, three major possibilities present themselves for companies that run Exchange:

- **Continue to operate an inhouse deployment of Exchange.** This includes variations such as traditional outsourcing to companies that operate Exchange either in your data center or theirs, or that place servers in client data centers and manage the servers remotely.

- **Embrace the cloud and move mailboxes to Microsoft Online Services.** You'll go through a migration phase to move mailboxes to the cloud, but eventually all inhouse mailbox servers that run Exchange will be eliminated unless you decide to keep some for specific user communities, such as executives. However, even if you move all mailboxes to online services, some inhouse servers will still be required to host Active Directory (AD) and to manage synchronization between the on-premise and online worlds, as well as other applications that don't function in the cloud.
- **Take a hybrid approach.** You'll move only those users to Microsoft Online Services who need the functionality delivered by a utility email service. You can then retain part of the current infrastructure to continue to run Exchange for specific user populations.

New companies that don't currently have an email system installed should absolutely consider cloud computing for email services, because this approach lets them start to use the latest version of email technology immediately. They can grow capacity on an on-demand basis and take advantage of the latest technology that's maintained by the service provider. Those who have an existing user base and a legacy IT infrastructure to deal with have some other problems to consider. For example, many large companies have integrated the provisioning of an email mailbox into their HR systems so that a mailbox and an email address are automatically created when new employees join. Processes like this take time to amend, especially when you deal with global companies that operate in multiple countries.

So What's in the Cloud?

One definition of cloud computing is "IT resources accessed through the Internet." Consumers have no obligation to buy hardware, pay software licenses, perform administration, or do anything else. They only need to have the necessary connectivity to the Internet to be able to access the service.

Cloud infrastructures are based on different OSs (Linux is a popular choice), but their operators put considerable effort into simplifying and securing the software stack that they use to drive performance and reliability. These infrastructures focus on scaling out rather than scaling up, preferring to use thousands of low-cost servers rather than fewer large servers. Applications are built using open standards such as SMTP, IMAP, POP3, and TLS so that as many users as possible can connect and use them. Google uses its own version of Linux running on commodity "white box" hardware, and its own file system, storage drivers, and applications to deliver a completely integrated and fit-for-purpose cloud computing platform.

In many respects, you can compare the integrated nature of Google's platform with that delivered by the mainframe or minicomputer in the 1980s and 1990s. As you'd expect, Microsoft's cloud platform is based on Windows, albeit with a high degree of attention to standardization and virtualization to achieve the necessary efficiency within the large data centers the company has built out in the United States and Ireland.

Why the Cloud Is Feasible

Over the past few years, technology advances have provided evidence to enterprises that including cloud platforms as part of their IT strategy is becoming an increasingly feasible and cost-effective strategy. Three examples of advances that have made cloud-based services more feasible are greater and cheaper access to high-quality Internet connections; the work done by companies such as Google to demonstrate that high-quality applications function on the cloud platform; and the growing comfort that users have on a personal level to store even their most personal data, such as family photographs or financial data, in sites such as Mint.com or Snapfish.com.

For Exchange, three developments are worth noting:

- **Advances in consumer experience.** Email applications such as Hotmail, Gmail, and Yahoo! Mail have created familiarity with the concept of accessing email everywhere through any device. Many people who use Exchange at work also have a free, web-based email account for personal email. These web-based providers run on a cloud platform, and while the majority of client access is through web browsers, some users connect to them with other clients, including Microsoft Outlook. Although service outages are possible with cloud-based providers, the overwhelming user experience is likely to be positive. Users get the feeling that if it's possible to host personal email in the cloud, it should be possible to host enterprise email, too.
- **The advent of RPC over HTTP.** The elimination of the requirement to connect to corporate email systems via VPNs demonstrates that it's possible to securely connect clients to email across the Internet. This capability has been available since Microsoft shipped Outlook 2003 and Exchange Server 2003, but Microsoft greatly improved the setup and administration of RPC over HTTP in Outlook 2007 and Exchange Server 2007. RPC over HTTP technology is now widely used, and Windows Server 2008 now includes the Net.TCP service to allow multiple services to share TCP ports for communication across HTTP.
- **Outlook running in Cached Exchange Mode.** Cached Exchange Mode is now the de facto deployment standard for Outlook clients. Cached mode insulates users from temporary network outages by letting them continue to work with a local cache that's constantly refreshed through synchronization with the server. Cached mode therefore helps enterprises maintain a high level of user confidence that they can continue to get their work done while connected to the Internet. Unlike carefully managed corporate networks, no one controls the Internet. Having the confidence that the Internet is sufficiently reliable to give clients consistent access to online services is of huge importance for companies when they consider moving away from on-premise services.

Economics of the Cloud

The trick that Microsoft now wants to perform is to transform part of its revenue stream into subscription services for access to applications such as Exchange, SharePoint, and Office Communications Server (OCS) without cutting its own throat by eliminating the rich stream of software licenses consumed for traditional inhouse deployment of these applications. At the same time, Microsoft knows that it has a huge competitor in Google, which has driven the market with Google Apps Premier Edition,

with a price point of around $60 per user, per year—which has attracted the attention of many CIOs, who now question how much they're paying for applications such as Exchange. Microsoft had to respond, and the company delivered in such a way as to be not only price-competitive but also feature-rich. Microsoft can't succeed against Google if its prices are way out of line, and it can't satisfy its customers unless the online versions of its applications offer comparable functionality to what customers have today. The coupling of Microsoft's price reduction for its online suite announced in November 2009 with the extra functionality enabled by Exchange 2010 ratchets up the competition between Microsoft and Google.

No administrator will be happy to upgrade clients without warning or consultation.

To achieve the necessary economics in the delivery of feature-rich applications at a compelling price point, the infrastructure to deliver cloud computing services is designed to scale to hundreds of millions of users, flexible in terms of its ability to handle demand, and to be multi-tenant but private. In other words, the same infrastructure can support many different companies, but an individual company's data is private and confidential. In addition, companies can have their own identity within the shared infrastructure. Microsoft has invested billions of dollars to build data centers in the United States and Europe to support the provision of online services to customers. According to Microsoft, as of November 2009, online services were available on a commercial or trial basis in 36 countries.

Exchange Upgrades

One advantage of online services is that online applications such as Exchange and SharePoint can be automatically updated to the latest version. You don't have to worry about testing and applying hotfixes, security updates, service packs, or even deploying a brand new release of Exchange. Everything happens automatically when Microsoft rolls out new software releases on a regular basis across its multi-tenant data centers.

Always having easy access to the latest application can be advantageous, but only if it doesn't increase costs by requiring client upgrades. For example, Exchange 2010 doesn't support Outlook 2000 clients; it requires you to use Outlook 2003 SP1 at a minimum. However, you need Outlook 2010 (which won't be available until sometime in mid-2010) to access the full range of features offered by Exchange 2010. Therefore, to move to a hosted service based on Exchange 2010, you have to be sure that all of your clients run either Outlook Web Access (OWA) or a client that's fully compatible with Exchange 2010. Outlook 2007 SP1 is the closest full-function client available for Exchange 2010 today.

You can predict that the same situation will continue to exist. OWA clients will be automatically upgraded in line with the server, but administrators will have to ensure that fat clients such as Outlook can connect. Microsoft typically provides backward compatibility only for recent clients, so client-side upgrades are always a possibility whether you use an inhouse or hosted version of Exchange. The problem here is that although you have complete control over upgrades when you run inhouse Exchange servers, you cede control to the hosting provider when you use an online service. If a hosting provider decides to apply an upgrade on its servers, there may be a domino effect requiring customers to either accept lower functionality or, in the worst case, not be able to connect with clients running on some or all desktops.

Managing Cloud-Based Deployments

Forced upgrades to new versions of desktop software might be an acceptable price to pay in order to take advantage of online services. However, no administrator will be happy to upgrade clients (or to even apply a service pack or hotfix) without warning or consultation. Particularly with bigger client populations in an organization, the costs to deploy or upgrade are larger, and it can be more difficult to ensure that all clients are running the right desktop software. A forced and unexpected upgrade at the wrong time could have enormous consequences for a business.

Through bitter experience, enterprise administrators have become aware of the need to synchronize client and server upgrades and to plan upgrades to match the needs of their organization. For example, it could be devastating to plan an upgrade to occur at the end of a fiscal year when users depend on absolute stability in their email system to send documents around, process orders, and finalize end-of-year results. Enterprise administrators also know about the other hidden costs that can lie behind client software upgrades. For example, you probably don't want to deploy Outlook 2010 without deploying the other Office 2010 applications because of the user interface changes that are common across the entire application suite. If you do, you'll automatically take a large hit on the time and testing needed to deploy. There is also the need to prepare users for the upgrade, and prepare your Help desk staff for a potential increase in workload and costs.

In an online world where services are truly utilitarian in nature, you might not have the luxury to dictate when client upgrades occur unless you use browser-based clients such as OWA. Consumer-oriented email services such as Hotmail and Gmail have always focused on web clients and therefore haven't needed to synchronize client and server upgrades. Perhaps we will all be able to use web clients in the future and eliminate fat clients such as Outlook. Until this happens online, service providers will have to work out how to perform software upgrades on their servers without forcing client-side upgrades on their enterprise customers.

Clients are only part of the management challenges that moving to an online service might pose for a company. In the second part of this article, we'll consider some other issues that may slow you down, such as compliance, legal issues, and managing service level agreements (SLAs).

InstantDoc ID 103110

Tony Redmond
(12knocksinna@gmail.com) is a contributing editor for *Windows IT Pro*, and author of *Microsoft Exchange Server 2007 with SP1* (Digital Press).

Find Files on Local Drives with Whereis.ps1

This PowerShell script supercharges the search capabilities of Get-ChildItem

by Bill Stewart

I often find it useful to search for files from a command line. In the past, I've typically used Cmd.exe's dir command with the /b and /s parameters to search for files; combining these parameters provides a list containing the full paths and filenames of matching files. However, dir doesn't have a simple syntax for searching multiple locations. For example, to search drives C and D for all files ending in .doc, you would use this command:

```
dir /b /s c:\*.doc d:\*.doc
```

The syntax gets even more complex when searching for multiple wildcard patterns (e.g., all .doc, .xls, and .ppt files) in multiple locations because you have to type each location and each wildcard pattern separately.

Windows PowerShell's Get-ChildItem cmdlet makes this task simpler. For example, to search drives C and D for all .doc, .xls, and .ppt files, you can use this command:

```
get-childitem c:\*,d:\*
  -include *.doc,*.xls,*.ppt -recurse
```

Get-ChildItem's first parameter is a list of paths to search, and the -Include parameter specifies a list of wildcard patterns that qualify the paths. The -Recurse parameter is analogous to the dir command's /s parameter.

Introducing Whereis.ps1

Although the Get-ChildItem cmdlet is quite powerful, I still found myself wanting additional functionality. For example, I wanted to be able to omit the -Recurse parameter and to automatically search local fixed drives if I didn't type a path. Before long, I began writing a full-featured script that augments the Get-ChildItem cmdlet with several additional features. The result is the Whereis.ps1 script, which you can download from *Windows IT Pro*'s website by going to www.windowsitpro.com, entering 103096 in the InstantDoc ID text box, then clicking the *Download the Code Here* button. (Note that the Whereis.ps1 script isn't an equivalent to the whereis command you might find on a UNIX-like OS.)

Whereis.ps1 uses the following syntax:

```
Whereis.ps1 -Name <String[]>
  [-Path <String[]>]
  [-LastWriteTimeRange <DateTime[]>]
  [-SizeRange <UInt64[]>] [-OneLevel]
  [-Files] [-Dirs] [-Force] [-DefaultFormat]
```

The -Name parameter specifies a wildcard pattern. This parameter's argument can be an array. Files and directories that match the wildcard patterns are included in the script's output. The -Name parameter is the only required command-line parameter. For information about the wildcard patterns you can use, enter

```
get-help about_wildcard
```

at a PowerShell prompt. Because -Name is a positional parameter, you can omit the parameter name (-Name) and type only its argument if it's the first parameter on the command line after the script name.

The -Path parameter specifies a path, and its argument can be an array. If you don't specify this parameter, Whereis.ps1 searches all local fixed drives. The -Path parameter is also positional, so you can omit the parameter name (-Path) and type only its argument if it's the second parameter on the command line after the script name.

The -LastWriteTimeRange parameter specifies an inclusive date range, and the argument can be an array. Items that have a LastWriteTime property within the range are included in the script's output. If you specify strings for this parameter's argument, Whereis

Table 1: -LastWriteTimeRange Parameter Examples

Range	Explanation
2008/01/01	Items modified January 1, 2008, and later
"Jan 1, 2007","Dec 31, 2007 23:59:59"	Items modified any time in 2007
0,"30 Jun 2008 11:59:59pm"	Items modified June 30, 2008, or earlier
0,((get-date) - (new-timespan -days 30))	Items modified 30 days ago or earlier
((get-date) - (new-timespan -days 30)),(get-date)	Items modified within the past 30 days

Table 2: -SizeRange Parameter Examples

Range	Explanation
32kb	Files 32KB in size or larger
0,32kb-1	Files smaller than 32KB
0,5gb	Files 5GB and smaller

.ps1 attempts to convert them to DateTime objects. If you specify a single date, Whereis .ps1 interprets the date range as "the specified date or later." If you specify an array, Whereis.ps1 interprets the first element in the array as the earlier date boundary and the second element in the array as the later date boundary. You can specify an "older than" date range by using zero as the first element in the array. Table 1 shows some examples for the -LastWriteTimeRange parameter.

The -SizeRange parameter specifies an inclusive size range, in bytes. This parameter's argument can be an array. Files that have a Length property within the range are included in the script's output. If you specify a single number, Whereis.ps1 interprets the range as "files of at least the specified size." If you specify an array, Whereis .ps1 interprets the first element in the array as the smaller size boundary and the second element in the array as the larger size boundary. You can also use PowerShell's numeric multiplier suffixes (kb, mb, and gb) when specifying the arguments for -SizeRange. Table 2 shows some examples for the -SizeRange parameter. Note that the -SizeRange parameter is ignored if you use only the -Dirs parameter (which I describe later), because directories don't have a Length property.

The -OneLevel parameter searches within the specified directories but not their subdirectories. That is, it's the inverse of Get-ChildItem's -Recurse parameter.

The -Files parameter causes Whereis.ps1 to include files in its output, and the -Dirs parameter causes Whereis.ps1 to include directories. The default is -Files. If you want to search for both files and directories, use -Files and -Dirs together. Use -Dirs by itself to search only for directories.

The -Force parameter corresponds to Get-ChildItem's -Force parameter. It causes Whereis.ps1 to search for items with hidden or system attributes.

The -DefaultFormat parameter causes Whereis.ps1 to output file-system objects instead of custom formatted string output. Figure 1 shows an example of Whereis.ps1's custom output, which is easier to read than if you output file-system objects, particularly if you have a large number of results, but you can't use the custom output as input for other scripts or cmdlets that expect file-system objects. The -DefaultFormat parameter helps you avoid this problem.

Inside Whereis.ps1

The param statement at the top of the script defines the script's command-line parameters. I typically use mixed-case variable names for script parameters (and other global variables) in PowerShell scripts, but this is only a convention and isn't required. After the param statement, the script declares the usage, isNumeric, writeItem, and main functions. Whereis.ps1 then calls the main function. Note that in PowerShell scripts, functions must be defined before they're called, which is why Whereis.ps1 doesn't call the main function until the last line in the script.

The usage function outputs a message explaining the script and how to use it, then exits the script. The main function calls the usage function if the -Name parameter is missing from the command line or if the -Help parameter is present.

The main function calls the isNumeric function to ensure that the arguments specified for the -SizeRange parameter are numeric. The isNumeric function works by using the -contains operator to see if its parameter's type is in the list of numeric types (e.g., Decimal, Double).

The writeItem function controls the format of the script's output. If the -DefaultFormat parameter exists on the command line, the writeItem function simply outputs its argument, which is a file-system object; otherwise, the function outputs a formatted string. It uses the standard .NET string formatting codes and the -f operator to produce the formatted string. For more information about string formatting, see the MSDN article "Formatting Types" at msdn .microsoft.com/en-us/library/fbxft59x .aspx.

The main Function

The main function, which Web Listing 1 shows (www.windowsitpro.com, InstantDoc ID 103096), contains the bulk of the script's code. The function's first job is to verify that the -Name parameter is present. If the -Name parameter is missing or if the -Help parameter is present, the main function calls the usage function, which outputs a usage message and ends the script.

The main function next converts the $Name variable into an array; the variable remains unchanged if it already contains an array. The function then uses a for loop to iterate the array. If an array element contains the * wildcard, it replaces the array with the $NULL value. This step is necessary to prevent the Get-ChildItem cmdlet, which runs later in the script, from outputting the

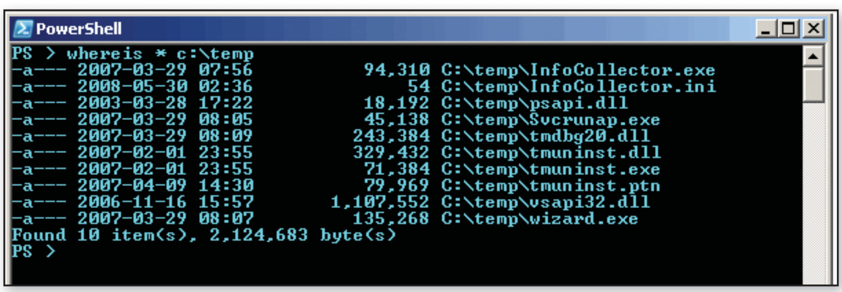


Figure 1: Sample of Whereis.ps1's custom output

contents of subdirectories underneath a directory.

Next, the main function checks to see if the -Path parameter is present. If the -Path parameter is missing, the function uses the Get-WmiObject cmdlet to retrieve a list of local fixed drives, as the code in callout A of Web Listing 1 shows. Therefore, the $Path variable contains either the path or paths specified with the -Path parameter or a list of local fixed drives. The main function then converts the $Path variable into an array; the variable remains unchanged if it already contains an array.

As the code in callout B shows, the function then uses a for loop to iterate the $Path array. For each element in the array, it checks whether the element ends with a backslash (\). If it does, the function adds the * wildcard to the path. Then the function checks whether the element ends with *. If it doesn't, the function appends *. When the for loop is complete, each element in the path array ends with *. This process lets us specify a path such as C:\Files, and the script interprets the path as C:\Files*. This script step not only saves typing when entering paths, but it's also required because the main function uses the Get-ChildItem cmdlet's -Include parameter. See the sidebar "Get-ChildItem's -Include Parameter" for more information about how the -Include parameter works.

The main function next determines if the -LastWriteTimeRange parameter exists. If this parameter doesn't exist, the function creates a two-element array. The function stores the earliest possible date (i.e., 1 January 0001, 00:00:00) in the first element, and it stores the latest possible date (i.e., 31 December 9999, 23:59:59) in the second element. The function gets the earliest and latest possible dates by retrieving the DateTime type's MinValue and MaxValue static properties.

If the -LastWriteTimeRange parameter exists, the main function converts the $LastWriteTimeRange variable into an array; the variable remains unchanged if it already contains an array. If the array contains only one element, the function appends a second element to the array containing the latest possible date. The main function next checks whether the array's first element is zero; if it is, the function uses the earliest possible date as the first element. Then the function attempts to convert both elements of the array into DateTime objects by using the DateTime type's Parse static method, as the code in callout C shows. If the Parse method throws an error, the script block following the trap statement runs, which outputs an error message and halts the script. The function then ensures that the first date is earlier than the second date; if this isn't true, the function throws an error, ending the script.

Next, the main function checks whether the -SizeRange parameter exists. If it doesn't exist, the function creates a two-element array, with a zero as the first element and the maximum value for a 64-bit unsigned integer (UInt64) as the second element. If the -SizeRange parameter exists, the function converts the $SizeRange variable into an array; the variable remains unchanged if it already contains an array. If the array contains only a single element, the function appends a second element to the array with the maximum value of the UInt64 type. The code in callout D shows how the main function then checks to see if both elements contain numeric values by calling the isNumeric function I described earlier. If either element contains a value that isn't numeric, the function throws an error, ending the script. The function also throws an error if the first array element is greater than the second element.

The main function then checks for the nonexistence of the -Files and -Dirs parameters. If neither parameter exists, the function sets $Files to $TRUE. It then sets two counter variables to zero: One to keep track of the number of items found ($count) and the other to accumulate the size of all files ($sizes).

At this stage, the main function has parsed and validated all of the script's parameters, so it executes the Get-ChildItem cmdlet. The function pipes Get-ChildItem's output to the ForEach-Object cmdlet so that it can perform further filtering for each object. If the -Files parameter exists and the object's PsIsContainer property is False (i.e., the object is a file and not a directory), then the main function checks to see if the object's LastWriteTime

Get-ChildItem's -Include Parameter

Get-ChildItem's -Include parameter serves as a selection pattern for the -Path parameter; only items in the specified path that match the -Include parameter's argument will be returned. However; you must specify a wildcard pattern or filename for the -Path parameter's argument for -Include to work. For example, the following command won't return any results even if you have a C:\Data directory that contains .txt files:

```
get-childitem c:\data -include *.txt
```

The command doesn't return any results because there's no wildcard pattern for -Include to qualify—it's simply a directory name without a filename pattern. You would use this command instead:

```
get-childitem c:\data\* -include *.txt
```

This behavior extends to the subdirectories of a directory if you use * with the -Include parameter. For example, consider this command:

```
get-childitem c:\data\* -include *
```

The * wildcard matches directories, too, so this command lists not only the files in C:\Data but also the contents of first-level directories under C:\Data. To list only the items in C:\Data, omit the -Include parameter or specify its argument as $NULL.

InstantDoc ID 103095

and Length properties are within the date and size ranges, respectively. If the object's properties are within specified criteria, the main function increments the $count and $sizes variables and calls the writeItem function to output the object. The main function performs similar checks to see if the -Dirs parameter exists and the object's PsIsContainer property is True (i.e., the object is a directory and not a file), except that it doesn't verify the object's size range or increment the $sizes variable because directory objects don't have a Length property.

Sample Commands

Now let's look at some commands that illustrate how to use Whereis.ps1 to perform various tasks. For instance, if you want to search for video and audio files on all local drives, you would use the following command:

```
whereis.ps1 *.asf,*.avi,*.mov,*.mp3,
  *.mp4,*.mpg,*.mpeg,*.qt,*.wav,*.wm,*.wmv
```

Note that although commands here are shown with line breaks for space, you would enter them all on one line; it's also important that you don't put spaces around the commas.

Next, to search for PowerPoint files that are 10MB or larger in C:\Data and its subdirectories, try this command:

```
whereis.ps1 *.pp[st]*
  C:\Data -sizerange 10mb
```

To search for files in C:\Data that have been modified within the past 60 days, use

```
whereis.ps1 * C:\Data
  -daterange ((get-date)
  - (new-timespan -days 60)),(get-
  date)
  -onelevel
```

If you want to delete all files in C:\Logs that were modified 30 days ago or earlier, you would use this command:

```
whereis.ps1 * c:\Logs
  -daterange 0,((get-date)
  - (new-timespan -days 30))
  -onelevel -defaultformat | remove-item
```

Get-ChildItem on Steroids

PowerShell's Get-ChildItem cmdlet has powerful native functionality, but Whereis .ps1 adds some useful functionality of its own. Add Whereis.ps1 to your toolkit and find what you're looking for even faster. Furthermore, you can build on the scripting concepts demonstrated here to customize and enhance your use of PowerShell cmdlets to suit your personal workload.

InstantDoc ID 103096

Bill Stewart

(bill.stewart@frenchmortuary.com) is a scripting guru and the lead IT analyst for French Funeral and Cremation Services in Albuquerque, New Mexico.

Essential SharePoint Security Practices: SharePoint Users and Groups

Secure your content through permissions management

by Randy Williams

A fundamental task for any IT administrator is security management, and security for Microsoft SharePoint is no exception. SharePoint, however, differs from most other IT systems. For example, SharePoint often grows organically, with little structure or governance. And executives usually want SharePoint to be flexible, enabling it to cater to the dynamic and evolving needs of the organization.

Another difference that makes securing SharePoint different from securing other systems is the idea of decentralization. Decentralization means you delegate security tasks to workers outside the IT group, such as content managers. This delegation might sound good, but it can introduce security risks. And if there's a problem, the IT guy usually gets the blame.

This introduction to SharePoint users and groups will help you manage permissions while maintaining a flexible yet secure SharePoint deployment. You'll learn how to break inheritance, how to create custom permission levels, and how to assign permissions to users or groups. I'll also offer recommendations to help ensure you're following the best practices based on your security needs.

Setting Permissions

A site collection is a hierarchy of websites, with each website containing lists and libraries that store content such as files, contacts, announcements, and web pages. A site collection defines a security boundary around this content so that users who have access to any content in a collection exist directly or indirectly as a site collection user. Administrators can grant users access to a site collection directly as a user, or indirectly through an Active Directory (AD) or SharePoint group. If you're using a custom authentication provider, you can also grant SharePoint access to your specific security principals. Whether users have access to all content in a site collection or a single document library buried deep within it, they are considered site collection users. Permissions in one site collection don't carry over to any other site collection, meaning each site collection is independently secured.

Permissions in a site collection behave similarly to NTFS permissions. By default, access permission in a site collection is inherited from the parent site. So, if Alice is granted read permissions at the top-level website in a site collection, this Read permission will cascade down to all content within the site collection. Similarly, if Alice is granted Read permission to a lower-level website, the permission applies only to this website and websites that fall under it.

Access to content is assigned through permission levels. Permission levels are combinations of individual permissions. An example of a built-in permission level is Contribute, which means a user has view, add, update, and delete access. You can also create custom permission levels as I explain shortly.

A user's actual permission is the sum of all permissions granted. So, if Bob has been granted Contribute and Design permission levels on a website, his effective permission will be both Contribute and Design.

Breaking Inheritance

Initially, SharePoint inheritance is in effect from the top of the hierarchy to the bottom for all content in the site collection. This means that you can change permissions only for the top-level website in the site collection. You can break inheritance by creating unique permissions at the website, list/library, folder, or item level. Figure 1 shows an example of a site collection hierarchy and permission inheritance.

To break inheritance, you first need to access the permissions page, which you can do as follows:

- For a website, go to Site Actions, Site Settings, Advanced Permissions.
- For a list or library, go to Settings, List (or Library) Settings, Permissions.
- For a folder or item, access the item's context menu, and click Manage Permissions.

From the permissions page, click Actions, Edit Permissions, and confirm the action by clicking OK. This will break inheritance and copy all the permissions down to the current level. It also establishes a new inheritance rule for this and lower levels. After inheritance is broken, you can reestablish it, but you'll lose any unique permissions that you created. To reestablish inheritance, click Actions, Inherit Permissions from the permissions page.

Creating a SharePoint Group

As with groups in other systems, SharePoint groups simplify permission assignments. You can place users, AD groups, or security principals from your custom provider into SharePoint groups. Note that although you can create a group within a sub-website, it will be stored in the top-level website. To create a SharePoint group, go to Site Actions, People and Groups. In the New menu, select New Group.

Granting Access to Users and Groups

You can assign permissions at the top-level website of the site collection or at any level at which inheritance has been broken. From the permissions page, select New, Add Users. Select the users or groups for whom you want to assign permissions and select the desired permission levels. In this context, groups can be AD groups or SharePoint groups. On this same page, you can also assign users to SharePoint groups; whatever permissions the group has will apply to the users. Note that SharePoint groups can't contain other SharePoint groups.

Creating a Custom Permission Level

Often, built-in permission levels aren't specific enough for your needs. For example, you might want users to have view, edit, and create permissions only. This permission level is similar to Contribute but without the ability to delete. Although you can change built-in permission levels (e.g., remove delete access for Contribute), it's not recommended. To create a new level, go to the permissions page as outlined earlier, and click Settings, Permission Levels, Add a Permission Level. You can also create a new permission level based on an existing one. Simply select the permission level from the Permission Levels screen. At the bottom of the page, click the Copy Permission Level button.

Understanding the All People Screen

The All People screen is one of the most misunderstood screens in SharePoint. The common misconception is that it represents all users that have some form of permission to content in the site collection. However, that's not true. To better understand, let's look at the three primary ways a user can appear on this list:

1. User was assigned direct permission at some level in the site collection. For example, Bob was granted Contribute permissions to Project A.
2. User was added into a SharePoint group within the site collection. For example, Alice was added to the Portal Members SharePoint group.
3. User was granted access through an AD group, and the user logged on to a website within the site collection and created or edited an item.

Deleting the user from the site collection doesn't necessarily remove access. Access removal works only if the user was assigned direct permission in the site collection. To remove user access granted via SharePoint

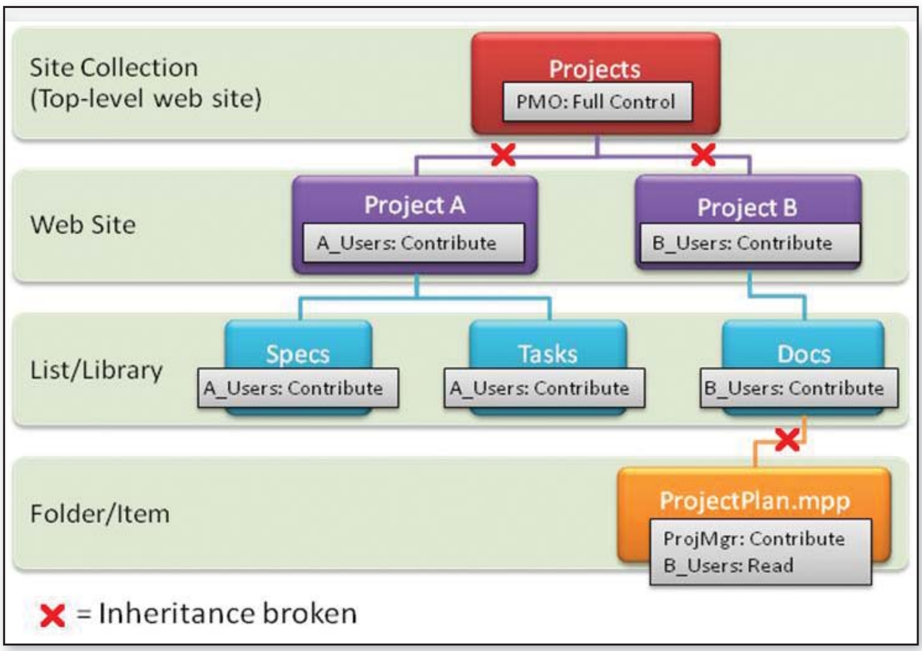


Figure 1: Permission inheritance

Learning Path

WINDOWS IT PRO RESOURCES

Get up to speed with SharePoint:

"SharePoint Server 2007 Unleashed," InstantDoc ID 94652

"SharePoint Server 2007 Revealed," InstantDoc ID 94914

Learn about SharePoint users and groups:

"SharePoint Solutions," InstantDoc ID 49234

"7 Things You Need to Know About SharePoint Services," InstantDoc ID 49873

or AD groups, you must remove the user from the group. Removing users from a group doesn't remove their names from the All People list; the list shows users who at some point had access.

Denying Access

Until now, I've talked only about granting access. What if you need to specifically prohibit a user from accessing content? Although this functionality is supported, you can't do it at the site collection level. You must do it at a higher level—the web application. By denying a user access at the web application, you deny access to all content in any site collection within that web application. To deny access, go into Central Administration. Click Application Management, Policy for Web Application. From this screen, select the desired web application. Next, select the users or AD groups and what type of deny permission you want. You can deny either write access or all access. Any policy set here will invisibly override any access granted at the site collection level and won't be seen within any site collection.

This screen is also where you can grant full read or full control permissions across all site collections in the web application. This option is useful for a legal team or auditors who need blanket access to all content. Again, this access is granted invisibly.

Changing or Reassigning Site Collection Administrators

A site collection administrator manages a site collection. This role often represents delegated users within the organization (not IT), who are responsible for managing and securing content. These users have full control permissions to all content within the site collection, even if inheritance is broken. When you create a site collection, you must specify at least one but no more than two users who will become the site collection administrators. An AD group can't be made a site collection administrator. If you need to change who the primary and secondary administrators are, go to Central Administration and click Application Management, Site Collection Administrators.

If you want more than two site collection administrators, you can add the users (or AD groups) to the SharePoint group called Owners, but keep in mind that permission inheritance can block access to these users. You can also grant them full control to the web application, as mentioned in the Denying Access section.

Let me also add that SharePoint has one or more farm administrators. These users, by default, don't have access to any site collection but are able to log in to Central Administration and add themselves as a site collection administrator. They can also change a web application's policy, so indirectly this is a powerful user.

By default, access permission in a site collection is inherited from the parent site.

Recommendations

Now that you understand the essential SharePoint security principles and how to perform several associated tasks, let me share some guidance and best practices in managing your permissions.

When to assign permissions to AD groups. If your organization already has a complete and accurate list of AD security groups that represents the roles in the organization, you should leverage these groups for SharePoint access. Simply add the AD group to a SharePoint group that represents the permission you want to grant. This is the most common form of access and the easiest to manage.

When to add users to SharePoint groups. Use this approach if your organization doesn't have well-managed AD groups or your site collection administrators have no easy way to adjust or request AD group membership changes. An example would be access to project-based websites where you create SharePoint groups for each project.

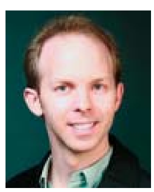
When to assign permissions to individual users. Individual permissions work well in special situations, such as for site owners, or for sensitive content, such as payroll data. These permissions are discouraged because it's more difficult to troubleshoot access or to duplicate access if one user leaves the company and is replaced by another.

Although SharePoint's security model is very granular, breaking inheritance and assigning new permissions throughout your site collections will quickly result in chaos. I recommend that you break inheritance only when necessary. You need to structure your content such that you can leverage inheritance as much as possible.

Unfortunately, permissions reporting (show me everything Alice has access to) or permissions duplication (grant Bob the same permissions as Alice) is lacking from SharePoint out-of-the-box. However, permissions reporting and permissions duplication can be achieved programmatically using the SharePoint object model. For information about the object model, see "Server and Site Architecture: Object Model Overview" at msdn.microsoft.com/en-us/library/ms473633.aspx. There are also many third-party utilities that help simplify these kinds of permission-management needs. Two good examples are Quest Software's Site Administrator for SharePoint and Lightning Tools' DeliverPoint.

Armed with these essential security principles, knowledge about how to perform permissions-related tasks, and best practice guidelines, you should be well on your way to delivering a secure, yet flexible SharePoint environment. And, let's hope a blame-free one as well!

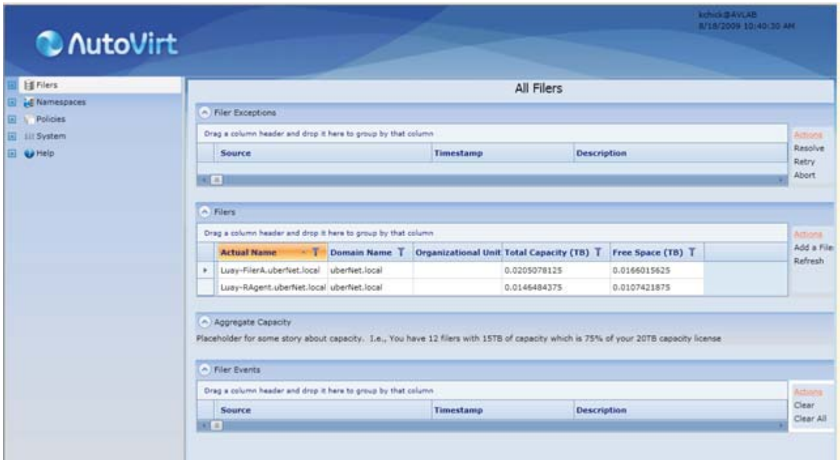
InstantDoc ID 103093



Randy Williams is a SharePoint Server MVP and senior consultant and trainer for Synergy Corporate Technologies, based in Singapore. He speaks about SharePoint topics at user groups and conferences and blogs at www.sharepointhawaii.com/randywilliams.

- Virtualization
- Systems Management
- SharePoint
- Email Archiving

AutoVirt 3.0 Aims to Clean Up Your Storage



AutoVirt 3.0 is a tool for managing unstructured data—anything that's not a database. According to the vendor, many companies add extra file servers because storage is so inexpensive. Staff at these companies must manually keep track of network paths, and because it's easier to add more servers than consolidate existing ones, they're not utilized fully. AutoVirt installs as three virtual machines and allows you, effectively, to treat all storage on your network as one drive, though it's also highly customizable, and allows you to specify which specific hardware will host which data. AutoVirt works in any size environment, but is targeting mainly at mid-size businesses—smaller businesses can often muscle through their storage problems manually, and enterprises usually have their own, much larger solutions. AutoVirt is available for Windows networks and costs about $25,000. To learn more, visit www.autovirt.com.

PRODUCT SPOTLIGHT

Citrix Makes NetScaler Virtual

Citrix announced today that its NetScaler appliance no longer has to have a physical presence in your data center with the release of a virtual version, **NetScaler VPX.** NetScaler started as a load balancer but it now also accelerates web applications' performance and provides security for them. Morgan Gerhart, senior manager of product marketing at Citrix, said the NetScaler appliance is in use by eight of the ten biggest websites.

Gerhart said that in the past, devices in the same class as NetScaler were fairly expensive, limiting the device to bigger companies. By going virtual, Citrix can offer NetScaler VMs for $2,000 to $30,000, not to mention a free limited version. As a virtual appliance, companies can better incorporate NetScaler functions into their development processes by giving access to NetScaler throughout the development process, instead of only on live systems. Gerhart said this could help eliminate common bugs that result from changes in the environment.

Another advantage of a virtual appliance is that its functions can be incorporated into cloud services. Citrix's release notes that two cloud services providers—SoftLayer and Joyent—already offer NetScaler to their customers, and more are expected to add it soon. So even small businesses and temporary sites can benefit from NetScaler, if they use cloud services. NetScaler VPX runs on standard X86 hardware. For now it runs on Citrix XenServer, but versions for VMware ESX and Microsoft Hyper-V are expected within a quarter or two. Visit www.citrix.com/netscalervpx for more information.

ScriptLogic Releases Desktop Authority 8

One of **Desktop Authority 8**'s biggest additions is machine-level management. With the new version, Desktop Authority can manage on both user and machine levels, so you can have "accounting machines" that get configured in a certain way, "accounting users" whose computers get configured a certain way, or a combination of both at once. Desktop Authority 8 also adds an improved Wake on LAN (WOL) function that uses agents on multiple subnets to send WOL packets. This works like a peer-to-peer network and is a better way to make sure your computers actually wake up for their maintenance. Desktop Authority 8 starts at $39, and an edition for users using System Center starts at $29. To learn more, visit www.scriptlogic.com.

Reduce SharePoint Content Database Size

BlueThread announces **StoragePoint for SharePoint 2010,** a product that reduces the size of SharePoint content databases by relocating content BLOBs out of the SQL Server database onto virtually any cloud-based or on-premise storage platform

Brian Reinholz | breinholz@windowsitpro.com
Editor's Note: Send new product announcements to products@windowsitpro.com.

and enabling the creation of policy-based storage profiles to manage content BLOBs at a very granular level. WSS 3.0 and MOSS 2007 customers can also install Storage-Point within their existing SharePoint deployment. Visit www.bluethreadinc.com to learn more.

Update Your Microblogging Network Within SharePoint

Present.ly, an enterprise microblogging platform developed by Intridea, announced the general availability of the **Present.ly SharePoint Web Part,** a free and open-source component that allows businesses to view and post updates to their company's microblogging network directly from within the SharePoint portal. Visit www.presently app.com to download the product.

UpdatePatrol Tracks SideWiki Sludge

Google SideWiki is Google's latest addition to the Google Toolbar—it creates a sidebar on every website where users can share comments and complaints about the site. Many businesses fear that competitors will use SideWiki to write negative and inaccurate comments about their products. To track comments made through SideWiki, consider using **UpdatePatrol.** Update Patrol is a program that lets you flag websites and web pages, and receive notification when those pages are updated with fresh content. (So it could be used to flag your favorite company and news sites, for instance.) And now, UpdatePatrol also supports SideWiki, so you can enter your own site, and then receive updates on SideWiki comments. UpdatePatrol costs $99.99 for a business user license—learn more at www .updatepatrol.com.

Manage E-Discovery Across Your Network

Discovery Attender is designed to pull together content in email archive, PSTs, across network file shares, and on local client drives for simple searching. The latest release, Discovery Attender 3.5, has been integrated with Sherpa Software's Archive Attender, creating a solution for email archiving and e-discovery in one. Discovery Attender's interface is wizard-driven and designed with nontechnical people in mind, letting you move search functions outside of the IT department. Discovery Attender 3.5 also adds the Combined Exception Log, which pulls together a list of any files the search is unable to access—for instance, something that's password protected—into a single list that you can act on. For more information, visit www .sherpasoftware.com.

Email Archiving Appliance Provides Turnkey Solution

With Gartner forecasting continued growth in the email archiving market, it's no wonder new vendors and solutions continue to emerge. MessageSolution and PineApp have just announced a partnership to provide a turnkey email archiving appliance, the **PineApp Archive-SeCure.** Based on MessageSolution's successful email archiving software, Archive-SeCure provides easy-to-implement and scalable email archiving for Microsoft Exchange Server, Lotus Notes/Domino, and just about any other type of mail server. Archive-SeCure can be purchased with internal storage or configured to access all types of external storage, and it uses file system architecture so there's no additional database to manage or license. All archived data is encrypted and compressed, providing security and reducing the storage footprint. Content indexing, including within attachments, allows for speedy searches, and single instance storage further reduces storage clutter. End-users and auditors can connect to the archive via a web-based interface, and management has a full set of auditing and logging capabilities for e-discovery and compliance. For more information about Archive-SeCure, visit www.pineapp.com website.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Windows 7

PROS: UI changes offer huge productivity wins for users; no major changes for those who deploy or manage Windows

CONS: Some UI tweaks feel half-completed; no antivirus bundled with the product

RATING: ◆◆◆◆◆

RECOMMENDATION: Windows 7 is the right product at the right time—an astonishing accomplishment when compared to Windows Vista. It's smaller, faster, simpler, and more focused than Vista. It's the first version of Windows to actually run better than its predecessor on the same hardware and to have lower real-world hardware requirements. A new taskbar with Jump Lists, interactive taskbar thumbnails, and other capabilities is the most obvious addition, and new window management methods like Aero Snaps, Aero Peek, and Aero Shake will make users more efficient. Windows 7 has it all. Highly recommended.

CONTACT: Microsoft • 800-426-9400 • www.microsoft.com

DISCUSSION: www.winsupersite.com/win7/review.asp

Microsoft My Phone

PROS: Free offsite phone backup makes losing or breaking current phone less painful

CONS: No integration with Microsoft's existing online services for contacts, calendaring, and storage; only 200MB of storage with no upgrades; requires Windows Mobile 6+

RATING: ◆◆◆◇◇

RECOMMENDATION: Microsoft My Phone is a free service that synchronizes contacts, calendar appointments, videos, text messages, documents and more between your Windows Mobile-based smart phone and your My Phone web account. The web service is ad supported, even if you pay for Hotmail Plus. While it's no reason to go the Windows Phone route, Windows Mobile device owners should take advantage of it.

CONTACT: Microsoft • 800-426-9400 • www .microsoft.com

DISCUSSION: www.winsupersite.com/mobile/myphone.asp

InstantDoc ID 103121

Double-Take Move

Like most IT pros, I've been involved in many hardware migration projects. After reading that **Double-Take Move** "revolutionizes the migration process with real-time data movement" (from Double-Take Software's website, www.doubletake.com/english/products/double-take-move), I wondered if this product could solve my migration woes.

Double-Take Move transfers data and workloads (defined as complete working systems with data) from one machine to another: either physical to physical, virtual to virtual, or any combination thereof. Think of the product as a very advanced Robocopy, Xcopy, or physical to virtual (P2V) migration tool. Double-Take Move isn't a replacement for Microsoft's Exchange Server and Active Directory (AD) migration tools. For example, you can't opt to move just Exchange mailbox data to another server without moving the whole Exchange server and its configuration at the same time. Double-Take Move works at the file-system level; it's not application-aware. After a Migrate Server operation, the target has the same OS, system state, data, applications, and configuration as the source server.

Workload Portability

Double-Take Move migrates workloads between physical or virtual servers by using a simple workflow through one console, with minimal interruption to end users. Double-Take Move works with Windows Server 2003 SP1 and later. An example use of Double-Take Move would be to migrate an operational instance of Small Business Server (the workload) to new physical hardware. Double-Take Move can also be used for migrating data between different storage solutions (e.g., from DAS to a SAN).

Double-Take Move can provision new virtual machines (VMs) on Hyper-V or VMware ESX Server, to which you can migrate existing physical or virtual workloads. If physical hardware is used as the target, the OS must be preinstalled. Although hardware doesn't need to be identically matched, the target server must have a similar configuration, and Double-Take Move performs the necessary checks before starting a migration job.

Preparing Source and Target Servers

In my testing, I moved a Windows 2003 file server to a physical target machine with Windows 2003 preinstalled. The source server was a member of my AD domain and the target a standalone machine. You prepare the source and target servers for migration by pushing an agent to both machines through the Double-Take Move console. The only prerequisite is that the .NET Framework 3.5 SP1 be installed on the source and target servers.

Double-Take Move features two migration options: Migrate Data and Migrate Server. Migrate Data includes all selected data; Migrate Server includes selected data plus the system state and installed applications. I created a Migrate Sever job, which was a simple task using the wizard. When the source and target servers have been specified and checked for suitability, you can set options for compression and bandwidth throttling for migrations over a WAN and for excluding unwanted files and folders. The wizard maps NICs between source and target servers when they're on the same LAN, and NICs in the target server will have their IP addresses changed at the end of the migration process. For WAN migrations, NIC settings remain unchanged and Double-Take Move renames the target server and updates DNS records accordingly. Multiple migration jobs can run simultaneously, and each job can be configured with email notifications if required.

Migration

When a migration job starts, data is synchronized from source to target server. After a full sync completes, changes to source data continue to be applied to the target server until you're ready to start using it. Users access the source server until you make the switch, at which time critical modifications are made to the target system, such as NIC configuration changes and share creation.

When you click Cutover in the console window, the source server shuts down and the necessary configuration changes are made to the target. After a reboot, the target server comes online as if it were the source. Users can then continue to access resources without any knowledge that the server is running on different hardware.

In my testing, the whole procedure worked flawlessly, with only a few minutes when I wasn't able to access resources due to the cutover. The target server successfully rebooted as a member of my domain and was configured identically to the source.

Risk-Free Migration

Changes to critical IT systems are risky, and none are more so than migration. Double-Take Move is an impressive, no-fuss solution that has all bases covered. It eliminates the hazards associated with migration to new hardware, using mature technology with support for locked files. It's hardware-independent and even captures NTFS alternative data streams and transactions.

InstantDoc ID 103092

Double-Take Move

PROS: Extremely simple to use and reliable; comprehensive network management for migrating workloads over WANs

CONS: Cost; intended for hardware, VM, and storage migrations only

RATING: ◆◆◆◆◆

PRICE: $495 per migration

RECOMMENDATION: If you need a proven system for migrating systems between physical or virtual servers, Double-Take Move provides an elegant means of transferring data, OSs, and applications with just a few minutes of disruption to availability.

CONTACT: Double-Take Software • www.doubletake.com • 866-474-5269

Russell Smith | rms45@rsitc.com

Mail Attender

Email administrators need to be able to search, report on, and control the information stored in their mail system. However, email servers don't always make this task easy—especially if users export and archive mail locally to PST files on their desktops.

Sherpa Software's **Mail Attender** is email management software that gives you control over email anywhere on your network, whether in Exchange Server mailboxes or public folders, or in PST files, either on file servers or local desktops. Mail Attender's rules-based architecture lets you define granular criteria to locate mail across all possible stores, then carry out a variety of actions, such as:

- Enforcing a corporate email policy throughout the organization
- Searching for inappropriate or sensitive content and potentially removing it
- Deleting old or large items to reclaim disk space
- Archiving and exporting mail
- Reporting on trends in mail volume or storage used

Installation and Setup

Mail Attender's installation process is straightforward. I particularly like the fact that although you can install the software on an Exchange server, it can also be installed on a standalone server. The product's documentation lists installation requirements; however, I would have liked more clarity about which prerequisites are necessary for the various supported OSs.

During installation, the software prompted me to install/update the Visual C++ 2008 Redistributable Package. Fortunately, this update is included and requires no additional downloads.

During setup, you must specify a user and mailbox for the processor service account to run under. Unfortunately, the documentation is focused on Exchange Server 2003 and Exchange 2000 Server rather than Exchange Server 2007. I had to figure out the Exchange 2007 permissions on my own.

Firing up the console reveals a relatively clean but dated interface, as you can see in Figure 1. The console is functional and easy to use, offering a multitude of ways to work with your email.

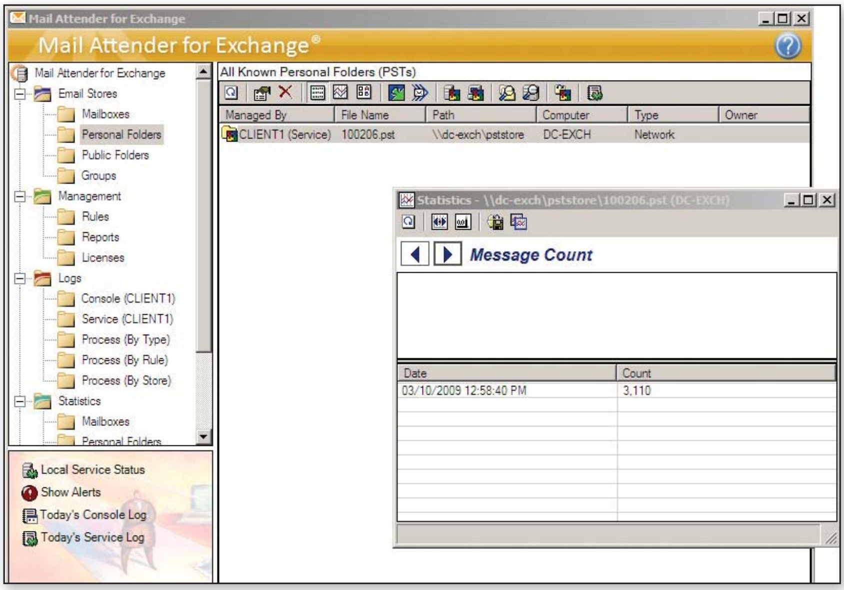


Figure 1: Mail Attender interface

The first task is to define the stores of mail to work with. You can select these stores in a variety of ways, including by Exchange server, direct from the Global Address List, or via Active Directory queries. You can specify just a single mailbox or public folder, multiple mailboxes or folders, or all mailboxes and folders. To access PST files for processing, Mail Attender scans a defined file share. To work with PSTs on desktops, you need to set up the server-based listener, which works in combination with a local processing engine that's installed on the desktop machine. Once the stores are set up, Mail Attender carries out automated scan jobs to keep up-to-date with any changes that occur.

After you define the stores to work with, you need to set up rules. The number of options is remarkable. There are three types of rules and predefined rule conditions and actions that allow for reporting about data, such as the size of Deleted Items folders, the space available on disks holding PST files, and the percent of quota a mailbox has used. In addition to passive reporting, the software offers wide-ranging actions such as moving large attachments, triggering external commands or programs, deleting mail, and flagging mail as important. You don't have to run all these rules yourself. Once you set up the rules you want, you can schedule them to run when necessary.

Another benefit is that you can run multiple instances of the processor on distributed servers. In addition, you can manage these instances locally and configure them to use a central SQL Server rules database.

Bottom Line

Despite the irritations of Mail Attender's interface and documentation, both of which need updating, the product has a lot going for it. Mail Attender has a massive number of conditions and actions with which to build rules, which lets you move, delete, and report on mail in almost any way you can think of—even across multiple mail systems. If you need a tool that gives you control over mail content no matter where it's stored, Mail Attender is certainly worth serious investigation.

InstantDoc ID 103152

Mail Attender

PROS: Easy installation; doesn't require installation on an Exchange server; numerous conditions and actions on which to build rules to manage mail; scales across multiple sites/systems

CONS: Dated interface; documentation needs updating for Exchange 2007 and later

RATING: ◆◆◆◆◇

PRICE: Starts at $19 per user

RECOMMENDATION: If you need a tool that gives you control over mail content regardless of where it's stored, Mail Attender is worth serious investigation.

CONTACT: Sherpa Software • 800-255-5155 • www.sherpasoftware.com

Nathan Winters | nathan@clarinathan.co.uk

Encore Electronics ENNUS1 Network Server

You probably think of USB as a standard interface for connecting peripherals to a single computer: You plug it in and use the resources, then unplug it when you're done. Typically, USB devices are non-shareable—unless you want to buy a costly, space-hogging, power-hungry hardware USB switch. Encore Electronics offers a nifty alternative.

Ideal for small-to-midsized businesses (SMBs) or home networks, the company's **ENNUS1 USB-over-Network Server** is a cool little device that lets networked users share access to USB devices. Do you have a USB all-in-one or multifunction printer (AIO/MFP) that you'd like to use across your network? How about a USB storage device such as an external hard drive, flash drive, or memory card reader? What about a USB scanner or webcam? You can simply attach the ENNUS1 device to your wired or wireless network, connect all the USB devices you want to share to the ENNUS1, and access those devices from anywhere in your environment.

Particularly for cash-strapped smaller companies, the ENNUS1 holds the potential for some cost savings in today's financial environment.

Installation of the ENNUS1 onto my network was a snap: After plugging the device into my wired/wireless router and attaching a USB hard drive and scanner to the ENNUS1, I ran the device's installation utility on two systems in my network: a primary server and a wireless client. On the first system, I opened up the ENNUS1 Control Center, which let me quickly connect to the ENNUS1 device and use the attached USB devices as if they were attached to the local system. The process was extremely quick and seamless. After repeating the utility installation on the laptop, that system also immediately recognized the networked USB hardware. However, to access the resources, I had to "disconnect" the device from the first system, then connect to it from the laptop. No two systems can access the same USB device simultaneously.

A technology called NetUSB—call it a "USB over IP" technology—transparently redirects USB packets to a TCP/IP network channel. The aforementioned "connect" and "disconnect" operations are merely software simulations. And although I had to manually connect and disconnect from the external USB hard drive, I found that the ENNUS1 provided automatic detection of my scanner. (The device offers the same automation for printers.)

The ENNUS1 is very easy to use, installing quickly and easily out of the box, but its GUI is a bit clunky. The interface uses a strangely abrasive clicking sound for UI navigation. Particularly for cash-strapped smaller companies, the ENNUS1 holds the potential for some cost savings in today's financial environment: There's no need to buy separate, expensive NAS enclosures or print servers. Your users will just have to become accustomed to the one-user-at-a-time connect/disconnect limitation. Another limitation: The ENNUS1 works only with Windows Vista/2003/XP/2000.

InstantDoc ID 103145

Encore Electronics ENNUS1 Network Server

PROS: Simple to use; quick installation; wired and wireless functionality; offers SMBs cost-savings potential

CONS: Clunky UI; connect/disconnect limits one user at a time to networked USB resources; works only with Windows Vista/2003/XP/2000

RATING: ◆◆◆◇◇

PRICE: $79.95

RECOMMENDATION: Consider this a measured recommendation. Despite some limitations, the ENNUS1 offers some clear benefits to smaller offices and home networks, particularly in this tough economy.

CONTACT: Encore Electronics • 626-336-4567• www.encore-usa.com

Jason Bovberg | jbovberg@windowsitpro.com

REDFLY Mobile Companion C8N

The Celio **REDFLY** is an interesting idea, and it's executed very well. It looks a lot like a typical netbook, only a little smaller, and weighs about the same as well. But the REDFLY can't do anything on its own. Instead, you tether your smartphone to the device using Bluetooth or USB. Your smartphone's display goes black (though the REDFLY has no speakers, so any sound will still come out of your phone) and the REDFLY's screen displays what you'd see on the phone's screen, larger and at higher resolution. You use the REDFLY's keyboard and trackpad to navigate.

Celio's tagline for the REDFLY is "Use your smartphone like a laptop," and it really delivers there, as long as your phone can handle it. For example, Microsoft Word on the REDFLY looked similar to a full-size version of Word, but there was a slight delay between when I hit a key and when the letter appeared on screen. When I tried Word on the same phone (an AT&T Tilt) without the REDFLY, however, I noticed exactly the same delay—it wasn't a problem with the REDFLY, but with the phone.

Microsoft Office and web browsers looked good on the REDFLY, but be cautious if you use your phone for other applications, because some can't handle the larger screen. The mobile Windows Media Player worked, but it took up only a small part of the REDFLY's screen instead of expanding to fill it. The phone's camera program wouldn't start while it was connected to the REDFLY, and several of the phone's included games had glitches that made them difficult or impossible to use on the REDFLY.

The REDFLY has a large battery capacity, and if you connect your phone with a USB cable, it can recharge your phone while letting you work with the larger screen. I plugged a phone with a nearly-dead battery into the REDFLY and left it running with the REDFLY's screen at normal brightness for about six and a half hours before the REDFLY ran out of juice.

Connecting the phone to the REDFLY was nearly seamless with both USB and Bluetooth. The only time I noticed anything other than instantaneous communication between the devices was when I tried to watch video over a Bluetooth connection and playback was choppy. Even with the phone about 20 feet away and on the other side of a wall, I was able to use the REDFLY to type a document in Word.

The REDFLY turns on almost instantly. With my test phone, it took about 7 seconds for the Bluetooth connection between the phone and the REDFLY to activate. Closing the lid of the REDFLY doesn't suspend it or turn it off like you might expect, but it turns on so quickly that you're free to hit the power button. The USB ports don't provide power while the REDFLY is turned off, though, so if you just want to recharge your phone, you'll have to leave the REDFLY on.

The REDFLY's keyboard is about the same size as the keyboard on typical netbooks. I found it a little uncomfortable for long stretches of typing, but I greatly preferred it to the phone's built-in keyboard. The REDFLY's trackpad is rectangular, compared to the more square trackpads on most laptops, but you can adjust its sensitivity and it generally performed well.

Celio plans to add support for BlackBerry and Android phones, but at press time REDFLY was compatible only with Windows Mobile 6.0 and 6.1 phones, and only certain hardware and software versions (check the list at www.celiocorp.com/smartphone). Windows Mobile doesn't have a very strong reputation at this time, so it's hard to recommend buying a compatible phone specifically to use with the REDFLY.

If you've already got a compatible phone, however, you should consider the REDFLY. It smoothly converts the tiny screen and keyboard of a smartphone into a netbook-like environment, provides extra battery life for your phone, and saves you from having to synchronize data between your phone and portable computer. As REDFLY adds support for more phones, it could become a must-have device for smartphone users.

InstantDoc ID 103060

REDFLY Mobile Companion C8N

PROS: Excellent connection technology; long battery life; small and lightweight

CONS: Performance is limited by Windows Mobile and phone hardware; limited phone compatibility

RATING:

PRICE: $249

RECOMMENDATION: If you've already got a compatible phone, the REDFLY is a great way to expand its capabilities. If not, carefully consider the limitations of compatible phones before choosing a phone/REDFLY combination.

CONTACT: Celio • 888-473-3359 • www.celiocorp.com

Zac Wiggy | zwiggy@windowsitpro.com

Netbooks IN THE ENTERPRISE

For one particular business user, netbooks might just be the ideal choice

by Paul Thurrott

Given the current economy, it's not surprising that the only growing segment of the PC industry is netbooks—small, lightweight machines that typically sell for less than $400. And it's natural to wonder whether low-cost netbooks might provide a viable alternative to traditional notebook computers in SMBs and perhaps even in the enterprise.

To determine whether netbooks make sense for you, you need to first understand exactly what a netbook is, how it fits into the overall PC market, and whether the upfront costs of such machines are matched by the long-term durability and manageability features that one should expect from a business-class machine. And since netbooks tend to ship with very low-end microprocessors and other low-end parts, you might have legitimate concerns about performance.

Netbook History

The first netbook—an ASUS Eee PC-branded portable computer—arrived in late 2007. Into the Eee PC's diminutive body, ASUS packed an ultra low-voltage (ULV) Intel processor, 512MB or 1GB of RAM, 2GB to 8GB of solid-state disk (SSD) storage (in lieu of a hard drive), and a 7" widescreen display running at 800 × 400. It also featured Wi-Fi networking, a full (if tiny) keyboard, and a traditional clamshell form factor. Although it was originally designed for the emerging computing market, the Eee PC rose to prominence when ASUS began offering it in the United States, following in the footsteps of One Laptop per Child (OLPC), which had also been offering a weird little low-cost, emerging-market notebook—the XO—to consumers in the United States. Interestingly, ASUS didn't market the original Eee PC as a *netbook*, but the term caught on as other companies entered the market and industry onlookers and PC makers tried to figure out a way to differentiate the devices from notebook computers.

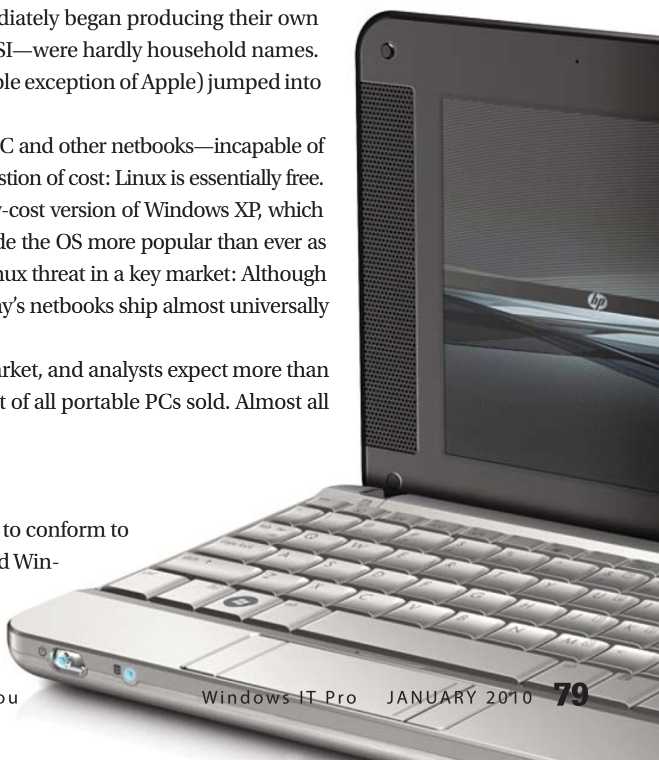
In fact, the Eee PC was so popular that other manufacturers almost immediately began producing their own low-end portable machines. The first few companies to do so—Everex and MSI—were hardly household names. But sensing a market opportunity, virtually all major PC makers (with the notable exception of Apple) jumped into the fray. They now all offer at least one brand of netbook.

The netbook's success was one of many affronts to Windows Vista. The Eee PC and other netbooks—incapable of running Vista—initially ran with a low-end Linux distribution, which led to a question of cost: Linux is essentially free. The popularity of Linux-based netbooks forced Microsoft to begin offering a low-cost version of Windows XP, which could run on the tiny Eee PC. This development extended XP's lifetime and made the OS more popular than ever as the fledgling netbook market took off. And Microsoft was able to stave off the Linux threat in a key market: Although virtually all netbooks sold through mid-2008 included some form of Linux, today's netbooks ship almost universally with XP.

Sales of netbooks rose exponentially the first few years they were on the market, and analysts expect more than 35 million of the tiny devices to be sold in 2009, adding up to about 20 percent of all portable PCs sold. Almost all these sales are to consumers—not businesses.

What's a Netbook?

To secure first XP and now Windows 7 at bargain pricing, PC makers have had to conform to a set of specifications when producing netbooks. (They're free to use higher-end Windows versions, of course, but they'll pay a lot more and have to pass that cost along to the buyer.) The result is that today's netbooks share numerous com-



mon features that truly do differentiate them from other low-cost portable computers.

Specifically, almost all netbooks now sold include a 1.3GHz, 1.6GHz, or 1.66GHz Intel Atom processor, 1GB of RAM, a 160GB (or smaller) hard disk, and a 10.1" (or smaller) display. Like notebook computers, netbooks have a clamshell form factor and feature wired and wireless networking functionality, two or more USB ports, VGA-out capability, and a full keyboard. Some netbooks include 3G wireless connectivity; indeed, some netbooks are now subsidized through wireless carriers with data plans, much like smart phones. Netbooks don't ship with optical drives—a drawback that can complicate software installation.

Intel's Atom processor is limited to 32-bit operation and can address only 2GB of RAM. As such, most netbooks can be upgraded to 2GB of RAM, providing excellent Windows 7 performance. But PC makers, to accommodate Microsoft's licensing requirements, don't ship netbooks with 2GB of RAM.

Most netbook differentiation today surrounds style and battery life. The typical netbook from mid-2009 could achieve roughly four hours of battery life, but MSI, Toshiba, and others are now shipping netbooks that can achieve eight, nine, or more hours of real-world battery life—good for all-day usage.

So, a netbook is easily defined, but its position in the market is decidedly more vague. Today's PC makers ship a variety of portable computers, including traditional notebook computers of various shapes and sizes, Tablet PCs, touch-compatible notebook computers, and even so-called smartbooks, which fit somewhere between smart phones and netbooks from a size and usage perspective. (A previous generation of smartbook computers was often referred to as the Ultra-Mobile PC—UMPC.)

However, the netbook's biggest looming competition is likely a generation of slightly bigger netbooks that have faster processors, more RAM capacity, and 11"-to-12" screens. These machines are simply notebook computers, of course, and will likely be marketed as such. But with better capabilities and only slightly higher price tags, traditional notebooks might eventually overcome the recent boom in netbook sales.

Do Netbooks Make Sense in Business?

Saving money is the top priority in most businesses, large or small, and that's truer than ever today. Looking at the current crop of netbook computers, it's possible to imagine them performing well in business scenarios, especially those machines (from top-tier PC makers) that feature longer-than-average battery life.

One revelation of the netbook era is that most users simply don't need high-end computers. Assuming the device is large enough to use comfortably, a standard netbook can handle virtually any office-productivity software, including Microsoft Office, web browsers, and email clients. From a performance standpoint, netbooks are less compelling for users who have high-end needs, but the needs of knowledge workers aren't typcially high-end.

Some other aspects of the netbook market make these devices less compelling for businesses. Netbooks' small screens (and onscreen resolutions) make them less than ideal for software such as Microsoft Excel and PowerPoint. The lack of an optical drive can make software installation difficult in smaller, less managed environments. And because most netbooks sell with a very low-end version of Windows 7, you'll need to upgrade the systems to more business-appropriate versions, such as Windows 7 Professional or Enterprise.

Durability is a concern, regardless of the make or model you're examining. PC makers large and small skimp on the components they use in netbooks because these devices sell for next to nothing and come with razor-thin margins. So, although it's possible to acquire, say, mainstream business notebooks with important reliability technology such as chassis roll cages, hard-disk suspension systems, and fingerprint-logon capability, netbooks from the same manufacturers feature none of these things. And they ship in cheap plastic bodies that degrade during the course of normal business travel.

Most important, perhaps, you won't find a netbook from any mainstream PC maker that's available through volume purchase and that comes with acceptable support. This void leaves out enterprises, but it should give pause to smaller businesses as well. Lenovo, for example, markets a diverse line of ThinkPad notebooks, Tablet PCs, and portable workstations to businesses. But if you're interested in the company's netbook products, your only option is the consumer-oriented IdeaPad line.

Businesses that do opt for netbooks will likely discover that the long-term costs of such machines will wipe out any up-front savings. These costs will include downtime for repairs, maintenance, and the cost of upgrading the hardware and software to meet the needs of users.

So, are netbooks a total wash in the business environment? Not quite. Netbooks are perfect for one particular scenario—and, not surprisingly, it's the scenario that matches the way that consumers are already using these devices. For employees who frequently work at home—including nights and weekends—netbooks might, in fact, make more sense than traditional notebooks or desktop PCs. The reason is that netbooks won't sustain the same level of abuse at home as they would on the road. And because netbooks are typically so cheap to acquire, and yet so popular with individuals, they'll be accepted by users quite readily.

Recommendations

Netbooks just don't make sense in most business environments, where their low durability and general unsuitability to the rigors of travel will prove problematic and overcome any upfront cost advantages. That said, netbooks do have their place in the broader PC market. If you run a smaller environment and need to accommodate users who work from home, netbooks are an interesting choice.

If you're choosing a netbook, be sure to choose a device from a major PC maker. Battery life won't be a significant problem for home users but should still be a concern as many users will prefer to be untethered for the day. Interestingly, the latest versions of the ASUS Eee PC line are still quite popular and meet these needs. But netbooks from Dell, HP, Lenovo, Samsung, and Toshiba are all highly recommended.

InstantDoc ID 103069

Paul Thurrott

(thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

iSCSI SANs

These storage options give you affordable high performance

by Zac Wiggy

Editor's Note: *Information in this Buyer's Guide comes from vendor representatives and resources and is meant to jump-start, not replace, your own research; also, some products might have been left out, either as an oversight or from lack of vendor response.*

You've probably noticed that your storage needs increase every day. Between email, databases, and applications, businesses of all sizes simply need to store more today than ever before. Luckily, storage prices continue to fall dramatically, so it's possible to keep up.

In businesses of all sizes, but especially small-to-midsized businesses (SMBs), iSCSI SANs gain more popularity every year, thanks in large part to their affordable prices. Entry-level iSCSI SANs are one of the fastest-growing areas, with these less-expensive options increasingly including features such as snapshotting and replication that were available only on high-end SANs in the past.

This month's buyer's guide table will give you an overview of the market. You'll see that the range of iSCSI options is huge, with some products priced at over $40,000 and some under $1,500, so make sure to consider your options carefully. Just as it's a big decision to go with iSCSI over alternative technologies, the level of iSCSI solution you decide to buy will have a big impact on how well it works for your environment.

iSCSI vs. DAS and Fibre Channel

DAS can be simpler than a SAN, especially at first, but DAS setups are limited by the amount of storage that can be attached to a single host. As you add more DAS storage, you have to deal with the infrastructure headaches that come from juggling the storage attached to separate servers. Multi-platform environments are another challenge for DAS—you have to make sure the Macs and Linux machines can share storage with your Windows machines.

Fibre Channel (FC) still offers better performance than iSCSI, but you'll definitely pay for that performance. FC has high implementation and support costs that tend to make it unpopular with SMBs. It's worth noting that while FC is still generally faster, the question of performance between iSCSI and FC isn't perfectly clear-cut. A few entries in our list support 10Gbps Ethernet, so iSCSI could get close to FC speeds, and the iSCSI protocol could actually give a slight speed advantage for certain workloads with small, block random I/O, such as virtualization.

iSCSI is something of a compromise compared with DAS and FC storage. DAS might be easier than iSCSI for relatively small amounts of data, but it's hard to scale up. FC provides the same kind of consolidated storage as iSCSI and will usually provide better performance, but costs more and has more complex hardware requirements. iSCSI hits a spot in between, being relatively inexpensive and providing good performance.

What You Need

There are plenty of factors to consider when choosing an iSCSI SAN. Some are obvious, but a few are tricky. Disk capacity is probably the simplest factor to take into account. Today's disk capacities would have seemed ridiculous just a few years ago—terabyte consumer-grade hard drives are now available for under $100, so it's no surprise that at the high end, iSCSI SANs are available with base capacities approaching 100TB and maximum capacities approaching a petabyte.

Don't be shortsighted when you're choosing how much storage to buy, but you don't have to be excessive either. One advantage of going with an iSCSI SAN is that you can add storage later. Be sure to check how scalable a SAN is before you buy it, because you could be able to defer some of your storage costs until you actually need the space.

Performance is also an important factor to consider. Not all iSCSI SANs support Serial Attached SCSI (SAS) drives, which are generally more expensive but faster than Serial ATA (SATA) drives. Some offer FC support, and a few have 10Gbps Ethernet support.

The buyer's guide table addresses many of the factors you should consider when choosing an iSCSI SAN, but remember to take into account the unique factors of your business. Power consumption is a factor for some companies. Hot swapping or adding drives could be more important for others. Your usage habits are unique, so fully understand what you need before you take the leap.

InstantDoc ID 103102

ZAC WIGGY (zwiggy@windowsitpro.com) is an assistant editor for *Windows IT Pro* and *SQL Server Magazine.*

ISCSI SANS

Company	Product	Price	Disk Capacity: Base	Disk Capacity: Total	Fibre Channel Support	Data Replication Support	Data Snapshot Support	Volume Shadow Copy Service (VSS) Support	Management Software
Dell 888-579-9762 603-579-9762 www.equallogic.com	EqualLogic PS6000	Starts at $17,000	2TB	768TB	No	Yes	Yes	Yes	Yes
	EqualLogic PS Series	$30,000	8TB	768TB	No	Yes	Yes	Yes	Yes
Dot Hill Systems 800-872-2783 www.dothill.com	Dot Hill 2332	$19,600	864GB	112TB	No	Yes	Yes	Yes	Yes
	Dot Hill 2330	$12,800	6TB	112TB	No	Yes	Yes	Yes	Yes
	Dot Hill AssuredSAN 2332ST	$25,600	12TB	96TB	No	Yes	Yes	Yes	Yes
Celeros 888-306-0646 650-325-6900 www.celeros.com	XD512	$42,750	96TB	512TB	Yes	Yes	Yes	No	Yes
	XD46S	$21,000	48TB	512TB	Yes	Yes	Yes	No	Yes
	XD11S	$3,750	4TB	24TB	No	Yes	Yes	No	Yes
D-Link Systems 800-326-1688 714-885-6000 www.dlink.com	xStack Storage DSN-5410-10	$18,500	Sold without drives	168TB	No	Yes	Yes	Yes	Yes
	xStack Storage DSN-5210-10	$14,000	Sold without drives	168TB	No	Yes	Yes	Yes	Yes
	xStack Storage DSN-3400-10	$16,500	Sold without drives	30TB	No	Yes	Yes	Yes	Yes
	xStack Storage DSN-3200-10	$6,000	Sold without drives	30TB	No	Yes	Yes	Yes	Yes
	xStack Storage DSN-2100-10	$4,930	Sold without drives	16TB	No	Yes	Yes	Yes	Yes
	xStack Storage DSN-1100-10	$1,800	Sold without drives	10TB	No	Yes	Yes	Yes	Yes
HP 866-447-7267 www.hp.com	HP StorageWorks X1000 Network Storage Systems	From $3,399	320GB SATA or 292GB SAS	12TB SATA	Yes	Yes	Yes	Yes	Yes
	HP StorageWorks 2000i G2 Modular Smart Array	From $4,999	7.2TB (24 × 300GB SFF SAS) or 12TB (12 × 1TB LFF SATA)	29.7TB SAS (99 × 300GB SFF) or 60TB SATA (60 × 1TB LFF)	No	No	Yes	Yes	Yes
	HP LeftHand P4000 SAN Solutions	From $30,000	4.8TB	192TB	No	Yes	Yes	Yes	Yes
Data Robotics 866-997-6268 408-567-3100 www.DataRobotics .com	DroboPro	$1,499-$3,499	N/A (bare chassis)	16TB	No	No	No	Yes	Yes

Data Protection Manager Software	Remote Management Capability	Hot-Swap Capability for Drives and Power Supplies	Fault-Tolerance/ Redundancy Support	Support for SATA/ SAS/Both	Thin Provisioning	Storage Pool	Speed and Number of Network Interfaces	Network Interface Teaming for Speed/ Redundancy
Yes	Yes	Both	Yes	Both	Yes	4 pools	4 × 1GbE or 2 × 10GbE per modular array; up to 16 arrays per SAN group	Both
Yes	Yes	Both	Yes	Both	Yes	4 pools	4 × 1GbE	Both
Yes	Yes	Both	Yes	Both	No	No	1Gb, 2 ports	Both
Yes	Yes	Both	Yes	Both	No	No	1Gb, 2 ports	Both
Yes	Yes	Both	Yes	Both	No	No	1Gb, 2 ports per controller	Both
Yes	Yes	Both	Yes	Both	No	Volume groups	6 × 1GbE or 4 × 10GbE or 4 × 8GbE FC	Both
Yes	Yes	Both	Yes	Both	No	Volume groups	6 × 1GbE or 2 × 10GbE	Both
Yes	Yes	Both	Yes	Both	No	Volume groups	2 × 1GbE	Both
Yes	Yes	Both	Yes	Both	No	Yes	One 10GbE port per controller provides full 1,160MBps line speed (purchase of separate XFP transceiver required)	Neither
Yes	Yes	Both	Yes	Both	No	Yes	Eight 1GbE RJ-45 ports per controller provide full 850MBps line speed	Both
Yes	Yes	Both	Yes	SATA	No	Yes	One 10GbE port provides full 1,160MBps line speed (purchase of separate XFP transceiver required)	Neither
Yes	Yes	Both	Yes	SATA	No	Yes	Eight 1GbE RJ-45 ports provide full 850MBps line speed	Both
Yes	Yes	Both	Yes	SATA	No	Yes	Four 1GbE RJ-45 ports provide full 425MBps line speed	Both
Yes	Yes	Drives only	Yes	SATA	No	Yes	Four 1GbE RJ-45 ports provide full 425MBps line speed	Both
Yes	Yes	Both	Yes	Both	No	Consolidate islands of DAS; can be file server, iSCSI target, or both	Minimum of two 1GbE NICs per model	Both
Yes	Yes	Both	Yes	Both	No	Consolidated storage array technology	2 × 1GbE ports per controller	Neither
Yes	Yes	Both	Yes	Both	Yes	Storage clustering allows consolidating multiple storage nodes into pools of storage	Two 1GbE or one 10GbE per SAN node; more nodes in a SAN cluster give higher aggregated network bandwidth	Both
Yes	No	Drives only	Yes	SATA	Yes	Up to 16 × 16TB smart volumes	1Gb iSCSI interface, 2 × Firewire 800, 1 USB 2.0	Neither

■ Exchange 2010 ■ Mobility ■ Networking

INSIGHTS FROM THE INDUSTRY

Exchange 2010: Helpful or Harmful for Third-Party Vendors?

Microsoft has added features to Exchange Server 2010 to make it more attractive to customers and give them more incentive to upgrade or switch from other vendors' products. But as is also typical, some of these features start to encroach on territory traditionally covered by third-party vendor products. The most notable example with Exchange 2010 is probably the new built-in email archiving functionality. The upside of this development cycle is the possibility for organizations to deploy Exchange with less need of additional support products and thereby save money. But that's not necessarily good news for the suppliers of those products.

Or so I thought, until I spoke with some of the vendors that currently have products that Exchange 2010's new features encroach upon. Robert Haaverson, CEO and CTO of Imanami, a company that provides group management features, talking about Microsoft's new release cycle, said, "The biggest innovations always come during these times." Haaverson takes new Microsoft developments as a challenge to improve Imanami's offerings. "It forces us third parties to build bigger and better things faster. We definitely can stay ahead of them. That's what third parties do," he said.

Exchange 2010 introduces new group management features such as the ability for end users to create and manage distribution groups. Commenting on this point, Haaverson said, "There's a gap between what [Exchange] 2010 does and what our product does. In other words, our product doesn't do everything that 2010 does. But there's a bigger gap between what 2010 does and what we do, meaning that our product does a lot of other things that Exchange 2010 can't do. So for a third-party vendor, it forces you to fix your negative gap—the part that they're ahead of you

> On one hand, Microsoft provides a new competitor, while on the other hand that competition provides impetus for innovation.

on—it forces you to fix that part first, and then build bigger and better things that go beyond their functionality."

Of course, the email archiving feature being introduced with Exchange 2010 isn't as fully featured as what you would find from any number of third-party vendors. In fact, the way Microsoft has implemented this feature, it really just appears to be a means of getting around the use of PSTs. It's controlled by end users, but the archive file is stored back on the same Exchange server, rather than on users' local drives. This architecture makes for easier backup and discovery, but critics say the extra data stored on the server can lead to reduced performance.

According to Ian Hameroff, a senior product manager with Microsoft, "We have a very strong belief that our customers get the best experience when the mail data is in Exchange. And our approach for archiving and retention and discovery keeps all that mail data in Exchange so we can deliver that full fidelity user experience and administrative experience. But at the same time, we also recognize that there may be some things that we don't do to the same extent, especially for complex compliance scenarios or regulations."

Hameroff and others at Microsoft continue to stress their commitment to working with third-party vendors to support Microsoft products. It even appears that there's a certain amount of planning for third-party support that's gone into the development of Exchange 2010. As Hameroff said, "We have our foundational capabilities built in to the product, and we have APIs that we're shipping—and we'll be shipping additional ones in subsequent milestones—that allow these third-party products to plug in and build on top of Exchange 2010."

So for the time being, Exchange 2010's built-in archive doesn't appear to be a serious threat to third-party email archiving vendors; other product areas might have somewhat greater challenges. Nonetheless, vendors and software developers who take on this challenge and use it to push their products forward, should continue to thrive. Most importantly, the ones that listen to their customers—the Exchange professionals in the field—and cater to their needs, should stay a step ahead of Microsoft in this constant chase.

—B.K. Winstead

InstantDoc ID 103055

Stop Throwing Away Money on Mobile Phones

Mobile phones are expensive. From smartphones to crummy "free with your plan" phones, it's a fact. On the business side, mobile phones are something of a necessary evil. Many cost-conscious organizations do what they can to reduce the number of employees with company-paid phones, but even so, there are positions that absolutely need them. Compass Management Consulting recently put out a white paper (compassmc.com/controls/insight.aspx?catid=3) that offers some advice for enterprises to significantly cut costs on company phones. I'll summarize the salient points below, along with what little personal insight I have to offer.

For businesses with 500+ devices, switching to a company-wide plan with one carrier will spell huge cost savings.

Enterprises: Switch to a Company-Wide Carrier!

For businesses with 500+ devices, switching to a company-wide plan with one carrier will spell huge cost savings. And, in addition to reducing the overall cost per person, this model will greatly simplify handling payments for all of these devices, plus provide much greater oversight into the mobile infrastructure of your organization. According to Compass, most enterprises have some devices under this type of model, plus some stragglers orbiting around the company outskirts if you will.

"Most typically, what we see happening is businesses creating a hybrid model where you have a large population of corporate-sponsored devices, typically BlackBerry devices centered around messaging, that type of thing, as well as some executive mobile phones," said John Lytle, lead consultant with Compass. "But then also, a large population of mobile devices, typically voice-type devices, that come in on expense reports, and just have no visibility from a management standpoint."

While it obviously varies significantly by company size, specific plans, etc., Lytle estimated that a company could go from $100 per device expense reimbursed to $70 per device in a corporate-sponsored system. One other really nice thing about this model is that minutes are pooled among all the phones, making overage charges a near impossibility.

Where to Start

Yeah, overhauling the whole company mobile setup could be a doozy. And if you have all these fragmented plans, you're going to have some that'll expire in six months and some that just started down the 2-year, soul-surrendering contract. For this situation, Lytle recommends overhauling as many to the new system as you can, and then continually adding new users as their contracts expire.

The other end to this whole equation is making the switch happen. I've summarized Lytle's response on how a company could go about that here: "First, you get the new strategy out there—socialize it in the enterprise and get people used to the fact that it's going to occur. Two is finding the inventory—so, trying to understand who has the devices, who's getting them put in through expense reports vs. who has corporate devices, so getting a hold of how big of an opportunity is this, and quite often that requires a corporate finance group to keep track of how many people are submitting phone bills each month.... Ultimately, there's a change in corporate policy—how are you going to pay for these devices, how are you going to provide them, and under what guidelines? Then you can get into leveraging types of plans and usage."

Thoughts for Smaller Organizations

Here's a few thoughts for how small to medium sized businesses can find some hidden cost savings.

- Check with your carrier of choice to see if there isn't still a managed model that could save you money. There's probably not much chance for an organization with five phones, but one with 100-500 might be able to use this model successfully still.
- Do a full inventory on all your phones with the following questions in mind: Do all of these employees need phones, and if so, do they need as robust of devices (such as smartphones), and are there any features I can remove?
- Make sure none of your employees are regularly going over their minutes, and formulate an immediate plan to nip that one in the bud.
- Talk to carriers and phone manufacturers to see if you can get bulk deals on new phones.
- Make a resolution to keep a watchful eye on your company's telecommunications spend. According to Lytle, some companies will spend as much as $500/month on one employee, between home Internet or phone service, work Internet and phone, plus mobile plans.

What are the biggest mobility headaches in your organization? Send me an email (breinholz@windowsitpro.com) or write to me on Twitter (twitter.com/breinholz).

—Brian Reinholz

InstantDoc ID 102941

Observer 14 Introduces Auto-Baselining and NetFlow Enhancements

I recently spoke with Douglas Smith, president of Network Instruments, about his company's release of Observer 14. The upgraded performance-management platform focuses on the most challenging problems IT pros face in quickly identifying and resolving application problems before they affect users. "Our main goal with the new version is to reduce the mean time to resolution," Smith says. "We want to give users a top-down view of their network so that when things turn red, they can quickly drill down to trouble areas."

Currently, companies are pigeonholed into one investigation pathway completely determined by their analysis tool. The newest Observer release expands these capabilities from a tool-centric to a solution-centric approach, giving network teams the freedom to set the investigation path, find the problem, and fix it. To that end, the Observer Reporting Server collects data from many data sources—whether they're Network Instruments probes, retrospective-analysis devices, or NetFlow devices such as routers or switches—and aggregates it into a global view from which you can drill down.

A nifty new feature of the Observer reporting Server is its auto-baselining capability. Smith says, "You can set up some criteria to compare today's data with data from the past. You can set criteria by a single day, or a day of the week, or a day of the month, for example. Is it deviating by a lot or a little?" Observer 14's auto-baselining lets you identify and respond to performance problems before they affect users. The platform automatically establishes baselines for all performance and time-based metrics. You can quickly determine whether application delivery or performance is acceptable based on current and past network traffic patterns. It allows for a more proactive approach to network management.

Overall, Network Instruments is starting to evolve from a network-centric view to an application-centric view of performance. "We're seeing that networks have different problems than they had a few years ago," Smith says. "Layer 2 or Layer 3 infrastructure has gotten pretty good. We're just not seeing the switching, addressing, and even cabling issues that we saw 10 years ago. The problems are in the higher layers—Layers 5, 6, and 7—so what we're seeing is corporations that want to look at application-level performance data in great depth."

Smith went on to describe the three areas of application analysis at which Observer 14 excels:

1. Application performance analysis—This is the transport. How fast does data get from point A to point B? "In an HTTP scenario, for example," Smith says, "this would be the tracking of the initial port opening. How fast did that happen?"

2. Application transaction analysis—This is the transported. What happened to the data before it got to the destination? Did the transaction complete correctly? "In the HTTP scenario," says Smith, "was there a page failure? Page not found? This is really the area where we feel Network Instruments is distinct from the competition."

3. Expert troubleshooting analytics—"This represents the 600+ conditions found by looking through data payloads," Smith says. "Observer 14 automates the sorting of that data."

Observer 14 brings other benefits, as well, including NetFlow scalability. "Observer Reporting Server can receive a flow from a router," says Smith, "and the router will report on all the traffic flowing through it. So it turns those Cisco devices into collection tools and they send out this formatted data. We've turned our GigaStor product into a NetFlow agent so it can send out the NetFlow stream to any reporting system."

The two clear advantages of this update: First, a number of security devices require NetFlows to work, and traditionally, if you don't have Cisco products, you're out of luck. But now you can install a GigaStor and provide that flow to the security products. Second, a limitation of NetFlow is that it shows only routed traffic—the traffic moving from one VLAN to another, not the traffic within a VLAN. GigaStor can now export that dataflow traffic within a VLAN. Smith says he's very interested to see how the marketplace reacts to this functionality.

You can find additional product information about Observer 14 at www.networkinstruments.com.

—Jason Bovberg

InstantDoc ID 103006

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support
Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/forums

News
Check out the current news and information about Microsoft Windows technologies.
www.wininformant.com

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- *asp.netNOW*
- *Exchange & Outlook UPDATE*
- *Office & SharePoint Pro UPDATE*
- *Security UPDATE*
- *SQL Server Magazine UPDATE*
- *WinDevPro UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services
Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Super CD/VIP
Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.
www.windowsitpro.com/sub/vip

Article Archive CD
Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.
www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections
Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

Office & SharePoint Pro
Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.officesharepointpro.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

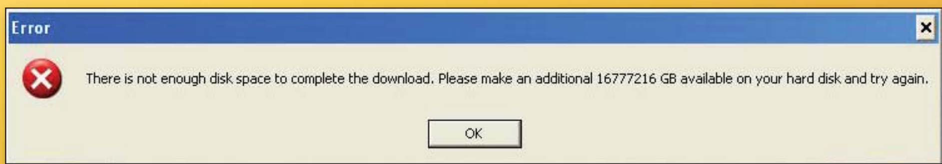
Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Regional Forums: We've introduced regional areas in our online forums, allowing IT user group leaders and other readers interested in meeting locally to more easily communicate with each other. Visit our forums at www.windowsitpro.com/forums and scroll down to see the new regional forums.

by Jason Bovberg

PRODUCT OF THE MONTH

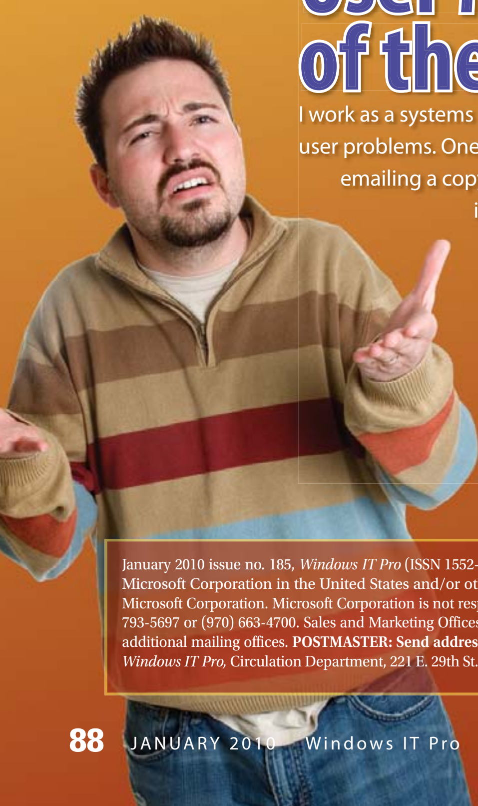
The UK company Thumbs Up has devised an aggravating little joke device that you'll almost certainly want to own. Simply plug in the PC Prankster to a work buddy's computer and it will take over the system, making random mouse movements, turning Caps Lock on and off, and typing garbage text and phrases. "Handily," says the Thumbs Up website, "the Prankster features a time delay setting, so that after installing it, you can make your getaway safely before it starts misbehaving." Your victim will find the PC Prankster quite annoying, but rest assured that it won't control the Enter key or close or save documents. Its point is to be mischievous—not dangerous. "However," says Thumbs Up, "it probably shouldn't be used on computers that control nuclear reactors, security systems for genetically recreated dinosaur parks, and/or zombie experimentation units, captured alien spacecraft, or freezers packed with delicious ice cream." Visit Thumbs Up at www.thumbsupuk.com.



No problem!

We imagine that Henrik is a busy man

User Moment of the Month



I work as a systems administrator for a high school, and I handle a lot of user problems. One day, a user complained that he was having difficulty emailing a copy of a book he'd written to his publisher. While speaking to him over the phone, I couldn't grasp why he was unable to attach the file to his message. When I went to see the problem for myself, I discovered that he had made each page of his book a separate Microsoft Word document—more than 70 pages. When I asked him why he didn't simply make one document, he shrugged and said, "I don't know." I stood there in disbelief for a moment, then zipped them all and sent them to the publisher to deal with.

—Benjamin Lambert

SEND US YOUR INDUSTRY HUMOR!

Email your industry humor, scandalous rumors, funny screenshots, favorite end-user moments, and IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive

A FREE GIFT.

January 2010 issue no. 185, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Copyright 2010, Penton Media, Inc., all rights reserved. Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries, and *Windows IT Pro* is used under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 221 E. 29th St., Loveland, CO 80538. Printed in the USA. BPA Worldwide Member.